#2
8-8-02

Docket No. 1359.1034

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Kazushi ISHIGAKI)
)
Serial No.: Not Yet Assigned)
)
Filed: December 22, 2000)

For: **ELECTRONIC COMMERCE SYSTEM AND METHOD**

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-191300
Filed: June 26, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By: _____
H.J. Staas
Registration No. 22,010

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500
Date: Dec. 22, 2000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　６月２６日

出願番号
Application Number: 特願２０００－１９１３００

出願人
Applicant (s): 富士通株式会社

２０００年１１月　６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９０３７０

【書類名】　特許願
【整理番号】　0095142
【提出日】　平成12年 6月26日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明の名称】　電子商取引システムおよび電子商取引方法
【請求項の数】　20
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　石垣　一司
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100095555
【弁理士】
【氏名又は名称】　池内　寛幸
【電話番号】　06-6361-9334
【手数料の表示】
【予納台帳番号】　012162
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9803089
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子商取引システムおよび電子商取引方法

【特許請求の範囲】

【請求項１】　利用者と業者の間の商取引を扱う電子商取引システムであって、

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記業者端末が備える、前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

前記業者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

第３者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項２】　利用者と業者の間の商取引を扱う電子商取引システムであって、

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

第３者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報とし

て付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項３】　利用者と業者の間の商取引を扱う電子商取引システムであって、

業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、

前記利用者端末が備える、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、

前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とした電子商取引システム。

【請求項４】　前記第３者機関が、前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うサイン認証部を備えた請求項１～３のいずれかに記載の電子商取引システム。

【請求項５】　前記電子透かし付与部が、前記電子サインデータを予め指定されたビット長の電子データに要約した要約情報を生成する電子サインデータ要約部を備え、前記商取引識別子に加えて前記要約情報も電子透かし情報として前記電子サインデータに対して付与する請求項１～４のいずれかに記載の電子商取引システム。

【請求項６】　前記電子透かし付与部は、前記業者端末を介した電子サインデータの送信があった場合に、登録されている利用者の連絡先データを基に利用者

に対して直接、該商取引における電子透かし付き電子サインデータ生成是非の確認を行う利用者確認部を備え、

前記利用者確認部は、前記利用者からの確認が得られない場合には前記業者端末に対して前記電子透かし付き電子サインデータの生成の拒否を通知する請求項１に記載の電子商取引システム。

【請求項７】　前記電子透かし付与部が電話通信手段と音声応答システムを備え、前記利用者の連絡先データが利用者の保持する携帯電話の番号であり、前記利用者確認部は、利用者が保持する携帯電話を介して前記利用者への前記確認内容を音声情報により問い合わせ、利用者確認を得ることを特徴とする請求項６に記載の電子商取引システム。

【請求項８】　前記電子透かし付与部が利用者の保持する携帯端末との通信手段を備え、前記利用者の連絡先データが利用者の保持する携帯端末のアドレス情報であり、前記利用者確認部は、前記携帯端末を介して前記利用者への前記確認内容を電子データとして問い合わせ、利用者確認を得ることを特徴とする請求項６に記載の電子商取引システム。

【請求項９】　前記商取引情報に基づいて、手書きサインによるサイン認証処理を省略するか否かを判定する手書きサイン省略可否判定部を備え、

前記手書きサイン省略可否判定部により手書きサインの省略が認められた場合、前記手書きサイン入力部による電子サインデータ読み取りと、前記電子透かし付与部による電子透かし付き電子サインデータの生成が省略され、前記商取引データ格納部に前記読み取った利用者識別情報と前記商取引情報を格納する請求項１～３のいずれかに記載の電子商取引システム。

【請求項１０】　利用者と業者の間の商取引の正当性を検証する電子商取引システムであって、

前記商取引の内容を表わす商取引情報を受け取る商取引情報取得部と、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る電子透かし付き電子サインデータ取得部と、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付

き電子サインデータ改ざんされているか否かをチェックする改ざんチェック部と、

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する商取引識別子抽出部と、

前記商取引識別子により一意に特定される商取引情報を、事前に真正な商取引情報が格納されている商取引情報格納部の中から取得する商取引情報検索部と、

前記商取引情報取得部と前記商取引情報検索部でそれぞれ得られた商取引情報を比較・照合する検証部とを備えた電子商取引システム。

【請求項１１】　利用者と業者の間の商取引を扱う電子商取引方法であって、

業者端末において利用者が提示した利用者識別情報を読み取り、

前記業者端末において前記商取引の内容を表わす商取引情報を提示し、

前記業者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取り、

第３者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、

前記第３者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項１２】　利用者と業者の間の商取引を扱う電子商取引方法であって、

業者端末において利用者が提示した利用者識別情報を読み取り、

前記業者端末において前記商取引の内容を表わす商取引情報を提示し、

前記利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取り、

第３者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得し、

前記第３者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデ

ータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項１３】　利用者と業者の間の商取引を扱う電子商取引方法であって、

業者端末において利用者が提示した利用者識別情報を読み取り、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取り、

前記利用者端末において、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成し、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納することを特徴とした電子商取引方法。

【請求項１４】　前記第３者機関において前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うことを特徴とする請求項１１～１３のいずれかに記載の電子商取引システム。

【請求項１５】　利用者と業者の間の商取引の正当性を検証する電子商取引方法であって、

前記商取引の内容を表わす商取引情報を受け取り、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取り、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックし、

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出し、

前記商取引識別子により一意に特定される商取引情報を、事前に格納されてい

る真正な商取引情報の中から検索し、

前記受け取った商取引情報と前記検索した商取引情報を比較・照合して検証することを特徴とする電子商取引方法。

【請求項１６】　利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと、

前記業者端末において前記商取引の内容を表わす商取引情報を提示する処理ステップと、

前記業者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子データとして読み取る処理ステップと、

第３者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得する処理ステップと、

前記第３者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項１７】　利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと、

前記業者端末において前記商取引の内容を表わす商取引情報を提示する処理ステップと、

利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る処理ステップと、

第３者機関において前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と前記利用者端末からの電子サインデータとを取得する処理ステップと

、

前記第３者機関において前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項１８】　利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

業者端末において利用者が提示した利用者識別情報を読み取る処理ステップと、

前記利用者端末が備える、前記業者端末から取得した前記商取引の内容を表わす商取引情報を提示する商取引情報提示部と、

利用者端末において提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る処理ステップと、

前記利用者端末において、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する処理ステップと、

前記業者端末において前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項１９】　前記処理プログラムが、前記第３者機関において前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行う処理ステップを備えた処理プログラムである請求項１６～１８のいずれかに記載のコンピュータ読み取り可能な記録媒体。

【請求項２０】　利用者と業者の間の商取引を扱う電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体であって、

商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取

引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る処理ステップと、

前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックする処理ステップと、

前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する処理ステップと、

前記商取引識別子により一意に特定される商取引情報を、事前に格納されている真正な商取引情報の中から検索する処理ステップと、

前記受け取った商取引情報と前記検索した商取引情報を比較・照合して検証する処理ステップを備えた処理プログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、クレジットカードやデビットカードなど利用者識別情報が記録された媒体を使用して、利用者が業者との間で商取引を電子データのやり取りにより行う、いわゆる電子商取引を行う電子商取引システムおよび方法に関する。特に、手書きサインを電子データとして利用し、該電子サインに電子的な透かしを埋め込むことにより、利用者側、業者側、双方の不正を防止・抑止する電子商取引システムおよび方法に関する。

【０００２】

【従来の技術】

クレジットカードを利用した商取引は、現在広く社会に普及しており、最近では利用者の銀行口座との間で即時に決済が行われるデビットカードも市場に導入され、ますます身近なものになってきている。このようなカードなど利用者識別情報を記録した媒体を用いる電子商取引では、真正の利用者であることを確認するために取引時に取引伝票に対して利用者のサインを筆記してもらい、これを業者側がカード背面の記入済の認証用の本人サインと比べることにより利用者が真正であることを確認し、利用者側のカードの不正利用を抑止するという方式が広く使われている。しかし、この方式では不正に他人のカードを入手した人が裏書

きのサインを練習して真似て筆記した場合には、特別に偽サインを見分ける訓練を受けていない人が偽サインであることを見破ることは難しいケースもあり、本人になり済ました偽サインによる不正使用を完全に防止することは難しい。また、利用者側からの万一のクレーム、取引内容の確認要求、取引監査に備えて、業者側は取引記録を残す必要があり、利用者がサインした紙の取引伝票を一定期間保管しているが、その保管に要する手間やコスト、取引伝票を検索する場合のコストも膨大である。

【０００３】

このようなカードの不正使用を抑止する技術として、あるいは、取引伝票の保管のコストを削減する技術として、筆跡照合技術を利用し、タブレットなどのペン入力装置を利用して入力された電子サインと、あらかじめ登録されている利用者の電子サインを照合して、利用者の本人認証を行い、カードの不正使用を抑止するシステムが提案されている。例えば、公開番号特開平１０－３２０４６５（カード与信・決済システム）には、業者端末が電子サインを入力する入力ボートを備えることによって、紙の取引伝票を不要にしてコストを削減する発明が開示されている。また、公開番号特開平１１－１４４０５６（電子署名照合方式およびシステム）には、電子的に入力された手書き署名（サイン）と登録済のサインデータを照合し、本人であるか否かを判定する技術が開示されている。電子サインを用いて本人認証を行う技術では、利用者の書き順や筆圧、筆記速度など、最終的な筆跡形状からは読み取れない情報を利用して認証を行うことができるので、不正利用者が筆跡をまねて練習しても、これらの非形状情報を含めて一致しない限り偽サインであると判定することができるので、不正防止効果が高いと言える。

【０００４】

これら従来の電子商取引方法を組み合わせたシステム構築例を図１１を参照しつつ説明する。

【０００５】

図１１において、５１０は業者側の店舗などに設置してある業者端末、５２０が利用者識別情報が記録された記録媒体であるカードを読み取るカード読み取り

装置、５３０が利用者が手書きサインを入力する電子タブレットなどの電子サイン読み取り装置、５４０が業者端末の制御部、５５０が業者側のサーバの記憶部内に設けられた取引情報を格納するための商取引情報格納部、５６０が手書きサインを基に利用者認証を行う認証センタが備える認証サーバ、５７０が認証サーバ５６０が備える利用者が真正サインとして登録した手書きサインを格納する登録サイン格納部、５８０が今回の商取引で入力された電子サインと登録サイン格納部５７０に格納された登録サインとの照合を行うサイン照合部、５９０が業者端末５１０と認証サーバ５６０の通信回線である。

【０００６】

商品などの購入の代金決済にあたり、利用者はカード読み取り装置５２０にクレジットカードなどを挿入して利用者識別情報を入力する。さらに利用者は電子サイン読み取り装置５３０を介して手書きサインを書き込み、電子サインとして入力する。業者端末５１０の制御部５４０は取得した利用者識別情報と電子サインを認証サーバ５６０に通信回線５９０を介して送信し、認証サーバ５６０はサイン照合部５８０において、入力された電子サインと登録サイン格納部５７０に格納された登録サインとの照合を行い、両者が一致すると判断した場合は、業者端末５１０の制御部５４０に対して利用者が真正のカード所有者であるとの利用者認証結果を報告する。業者端末５１０は商取引終了後、商取引に関する情報を業者側サーバ内の商取引情報格納部５５０に格納する。もし、サイン照合部５８０において電子サインが不正であることが疑わしい場合には制御部５４０に対して利用者認証ができなかった旨を報告する。業者端末５１０は当該取引を拒否したり、警告を発したり、または利用者にサインの再入力を促すなどの処理を行うことができる。上記の構成によれば、カードの不正利用を抑止することができ、また、取引情報を従来の紙媒体の取引伝票に代え、電子サインとともに業者側端末の記憶手段に電子データとして記憶することができ、紙伝票の保管コストや監査時の伝票検索コストなどを削減することができる。

【０００７】

【発明が解決しようとする課題】

上記従来技術のように、カード取引時の手書きサインを電子化した電子サイン

とすれば、本人の登録サインと、商取引ごとに入力された電子サインとを、利用者の書き順や筆圧、筆記速度など、最終的な筆跡形状からは読み取れない情報を利用して認証を行うことができ、利用者側の不正使用を抑止する効果が高くなるほか、保存するデータが電子データであるので業者側の取引伝票保管に関するコストを大幅に低減することができる。

【０００８】

しかしながら、利用者側から見れば、自分の手書きサインが電子データとして業者側端末に取り込まれて保管されることとなり、業者側の悪意のサイン盗用、架空取引へのサイン複製、流用などの不正利用の可能性が大きくなりセキュリティ上の問題が発生する。つまり、利用者のサインが電子データとして業者端末に取り込まれるため、簡単に電子サインデータを盗用、複製することができ、業者側によって当該利用者の電子サインが悪用され、実際には行われていない架空取引に使われるなどの危険性を否定できない。

【０００９】

本発明の電子商取引システムおよび電子商取引方法は、取引伝票を電子化した商取引情報に対して電子的に入力された電子サインの単なる付加による利用者認証に代え、当該電子サインが、取引業者や第三者によって盗用、複製されることを防止し、架空取引などに悪用されることを効果的に防止した電子商取引システムおよび電子商取引方法を提供することを目的とする。

【００１０】

さらに、従来の紙媒体の取引伝票に対する手書きサインによる利用者認証に比べ、認証精度が高く、かつ、取引業者の取引情報の保存コスト、検索コストを低減する電子商取引システムおよび電子商取引方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記課題を解決するために、本発明の電子透かし付き電子サインを用いた電子商取引システムは、利用者と業者の間の商取引を扱う電子商取引システムであって、業者端末が備える、利用者が提示した利用者識別情報を読み取る利用者識別情報読み取り部と、前記業者端末が備える、前記商取引の内容を表わす商取引情

報を提示する商取引情報提示部と、前記業者端末が備える、提示された前記商取引情報に同意した利用者が入力する手書きサインを電子サインデータとして読み取る手書きサイン入力部と、第３者機関が備える、前記業者端末から商取引の内容を示す商取引情報と利用者識別情報と電子サインデータを取得し、前記電子サインデータに対して該商取引を一意に特定する商取引識別子を電子透かし情報として付与し、電子透かし付き電子サインデータを生成する電子透かし付与部と、前記業者端末が備える、前記電子透かし付き電子サインデータを取得して前記商取引情報とともに格納する商取引データ格納部とを備えたことを特徴とする。

【００１２】

上記構成により、商取引に関する情報の保存および管理が電子データの形で行うことができ、取引の利便性が高まり、データの保存コスト、監査時の検索コストの低減も可能となる。また、電子透かし付き電子サインを埋め込んだ電子透かし付き電子サインデータを生成するので、業者による電子サイン盗用防止および悪意の架空取引への流用が防止できる。また、電子透かし付与部が利用者および事業主体とは異なる第三者機関が管理・運用しているのでカード不正利用、業者側の手書きサイン盗用、架空取引への流用に対するセキュリティが向上する。

【００１３】

なお、上記構成では、手書きサイン入力部を業者端末に設ける構成としているが、該構成に代え、利用者端末に設ける構成とすることも可能である。

【００１４】

この構成によれば、手書きサイン入力部が利用者端末に設けられているので、業者端末に設けた構成よりもさらに業者による電子サイン盗用防止および悪意の架空取引への流用を防止するセキュリティが高まり、さらに、利用者が電子サインを入力することへの抵抗感が薄まるという心理的効果も期待できる。

【００１５】

なお、上記構成では、電子透かし付与部を第３者機関に設けた構成としているが、該構成に代え、利用者端末に設ける構成とすることも可能である。

【００１６】

この構成によれば、電子透かし付与部が利用者端末に設けられているので、電

子透かし付与処理に対する利用者確認を不要とすることができる。

【００１７】

また、第３者機関が、前記利用者識別情報を基に予め登録されている前記利用者の真正サインデータを検索し、該真正サインデータを用いて前記電子サインデータの照合・認証を行うサイン認証部を備えることが好ましい。

【００１８】

上記構成により、商取引の際に、電子サインデータと真正サインデータを用いた利用者の認証を実行することができ、商取引のセキュリティがさらに向上する。

【００１９】

次に、本発明の電子商取引システムにおいて、前記電子透かし付与部が、認証された電子サインデータを予め指定されたビット長の電子データに要約した要約情報を生成する電子サインデータ要約部を備え、前記商取引識別子に加えて前記要約情報も電子透かし情報として前記電子サインデータに対して付与することが好ましい。

【００２０】

上記構成により、電子透かし情報として前記商取引識別子に加え、電子サインデータから一意に生成される要約情報を付与することができるため、電子サインの偽造に対するセキュリティがさらに向上することとなる。

【００２１】

また、本発明の電子商取引システムにおいて、前記電子透かし付与部が、前記業者端末を介した電子サインデータの送信があった場合に、登録されている利用者の連絡先データを基に利用者に対して直接、該商取引における電子透かし付き電子サインデータ生成是非の確認を行う利用者確認部を備え、前記利用者確認部は、前記利用者からの確認が得られない場合には前記業者端末に対して前記電子透かし付き電子サインデータの生成の拒否を通知することとすれば、商取引の成立の前に、第三者が介在しない形で事前に利用者に対して利用者確認を得ることができ、利用者からの確認が得られない場合には、電子透かし付き電子サインデータの生成の拒否を通知することができ、セキュリティを高く維持することがで

きる。

【００２２】

また、上記電子商取引システムにおいて、前記商取引情報に基づいて、手書きサインによる認証処理を省略するか否かを判定する手書きサイン省略可否判定部を備え、前記手書きサイン省略可否判定部により手書きサインの省略が認められた場合、前記手書きサイン入力部による電子サインデータ読み取りと、前記電子透かし付与部による電子透かし付き電子サインデータの生成が省略され、前記商取引データ格納部に前記読み取った利用者識別情報と前記商取引情報を格納することも可能である。

【００２３】

この構成によれば、商取引のセキュリティレベルが低くなるが、商取引の金額・種別などによっては商取引処理手続を簡略化しても実運用上に耐え得ると扱える場合では問題とはならず、商取引の処理内容を低減することができるので処理の効率化を図ることができる。

【００２４】

次に、本発明は、商取引完了後に決済機関側や業者側で過去の該商取引情報の真正性が問題となった場合などに商取引内容の検証を行うシステムも提供する。利用者と業者の間の商取引の正当性を検証する電子商取引システムであって、前記商取引の内容を表わす商取引情報を受け取る商取引情報取得部と、商取引に用いられた電子サインデータに対して該商取引を一意に特定する商取引識別子が電子透かし情報として付与された電子透かし付き電子サインデータを受け取る電子透かし付き電子サインデータ取得部と、前記電子透かし付き電子サインデータの電子透かし情報を調べ、電子透かし付き電子サインデータ改ざんされているか否かをチェックする改ざんチェック部と、前記電子透かし付き電子サインデータの電子透かし情報から商取引識別子を抽出する商取引識別子抽出部と、前記商取引識別子により一意に特定される商取引情報を、事前に真正な商取引情報が格納されている商取引情報格納部の中から取得する商取引情報検索部と、前記商取引情報取得部と前記商取引情報検索部でそれぞれ得られた商取引情報を比較・照合する検証部とを備えたことを特徴とする。

【００２５】

上記構成により、入力された検証が求められている商取引情報と、別途格納されている真正の商取引情報の中から電子透かし付き電子サインデータを基に一意に特定された真正の商取引情報とを比較し、当該検証が求められている商取引情報が真正であるか否かを検証することができる。

【００２６】

本発明の電子透かし付き電子サインを用いた電子商取引システムは、上記の電子透かし付き電子サインを用いた電子商取引システムを実現する処理ステップを記録したコンピュータ読み取り可能な記録媒体から処理プログラムを読み込むことにより、コンピュータを用いて構築することができる。

【００２７】

【発明の実施の形態】

本発明の電子商取引システムおよび電子商取引方法の実施形態を以下に示す。以下では、典型例として店頭でのクレジットによる商品購入の商取引に適用した例を説明するが、本発明はサインが本人認証に用いられるアプリケーションに対して適用可能である。

【００２８】

（実施形態１）

実施形態１の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。

【００２９】

図１は、実施形態１の電子商取引システムの構成例を示すブロック図である。

【００３０】

図１において、１０は業者端末、２０は利用者識別情報読み取り部、３０は手書きサイン入力部、４０は業者端末の制御部、５０が商取引データ格納部、６０がデータ送受信部である。本実施形態１の構成では、業者端末１０が手書きサイン入力部３０を持った構成であり、当該手書きサイン入力部３０が商取引情報提示部３１を備えている。

【００３１】

１００は第三者機関である電子サイン管理機関が管理する電子サイン管理サーバである。電子サイン管理サーバ１００は、データ送受信部１１０、電子透かし付与部１５０、商取引管理データ格納部１６０を備えている。なお、本実施形態１では、業者端末１０が取引内容入力部１１を備え、電子透かし付与部１５０が、電子透かし情報取得部１５１、電子サインデータ要約処理部１５２、電子透かし付与処理部１５３、利用者確認部１５４を備えた構成となっている。

【００３２】

２００は決済機関のサーバである。決済機関のサーバ２００は、商取引情報生成部２１０を備えている。ここで、決済機関と電子サイン管理機関は、利用者や業者とは異なる第三者機関とする。なお、決済機関と電子サイン管理機関は、別機関であっても良く、同じ機関が兼ねるものでも良い。ただし、また、商取引情報生成部２１０は電子サイン管理サーバ１００内に備える構成としても良い。

【００３３】

３００はネットワークであり、電話回線やインターネットなどである。４００は利用者が携帯している携帯電話などの携帯端末である。

【００３４】

図１に示した構成要素を簡単に説明する。

【００３５】

業者端末１０は、業者の店舗内に設置された端末で電話回線やインターネットなどにより決済機関のサーバ２００や電子サイン管理機関の電子サイン管理サーバ１００と接続されている。

【００３６】

取引内容入力部１１は、業者が商取引に際して、商品の代金、商品コードなど取引内容に関する情報を業者端末１０に入力する部分であり、例えば、業者店舗に設置されているレジスタやＰＯＳ端末から入力された商品の代金、商品コードなど取引内容に関する情報を業者端末１０に送信する構成でも良い。

【００３７】

利用者識別情報読み取り部２０は、利用者識別情報を読み取る部分で、利用者識別情報を記録した記録媒体に応じて様々な形態がある。例えば、磁気ストライ

プ付きカードであれば、カードの磁気ストライプリーダとなり、ＩＣカードであれば、ＩＣカードリーダとなり、また、暗証番号（ＰＩＮ番号）が併用される場合にはＰＩＮ番号入力テンキーが備えられる。指紋や声紋などバイオメトリック情報を利用する場合は、それら情報を読み取る専用デバイスが搭載される。

【００３８】

手書きサイン入力部３０は、手書きサインを電子データとして読み取る部分であり、例えば、電子タブレットなどである。電子データ化できるものであれば、電磁誘導式タブレット、感圧式タブレット、光学式タブレットなど種類の如何を問わないが、最終的な筆跡形状のみならず、利用者の書き順、筆圧、筆記速度など手書きサインに関して照合に用いる多様な情報を読み取れることが好ましい。

【００３９】

商取引情報提示部３１は、利用者がサインするにあたり、商取引内容である商取引情報を確認するために該情報を利用者に提示する部分である。ここで、商取引情報とは、業者番号、業者伝票番号、取引金額などを含む商取引内容を表わす情報であり、特に、取引金額は業者による改ざんを防止する目的から商取引情報に必須の情報とする。本実施形態１の構成では商取引情報は決済機関のサーバ２００が備える商取引情報生成部２１０により生成される。生成に際しては業者端末１０において取引内容入力部１１を介して入力された取引内容を示す情報、利用者識別情報読み取り部２０を介して読み取られた利用者識別情報が決済機関のサーバ２００に送信され、決済機関のサーバ２００においてそれら情報を基に商取引情報が生成される。従来の紙伝票処理におけるサインが空欄状態の伝票にあたる。利用者は商取引情報提示部３１が提示した商取引情報の内容を確認して同意すれば手書きサイン入力部３０を介して手書きサインを入力する。ここで、商取引情報提示部３１が手書きサイン入力部３０の電子タブレットなどを利用して商取引情報を提示する構成とすれば、電子タブレット上に提示された商取引情報のサイン欄に手書きサインを入力するという運用が可能となる。

【００４０】

業者端末の制御部４０は、業者端末１０の動作を制御する部分である。

【００４１】

商取引データ格納部５０は、商取引が成立し、完了した後、電子透かし付き電子サインデータを格納・保存する部分である。

【００４２】

データ送受信部６０は、電子サイン管理サーバ１００や決済機関のサーバ２００との間でデータの送受信を行う部分で、通信インタフェースを備えている。

【００４３】

次に、決済機関のサーバ２００を説明する。決済機関のサーバ２００は、クレジット会社や銀行などの決済機関が管理するサーバであり、決済に関する信用保証を行う処理を行う。決済機関のサーバ２００は商取引情報生成部２１０を備えている。業者端末１０から送信された取引内容を示す情報と利用者識別情報を基に商取引情報が生成される。信用保証は商取引情報に真正と判定された電子透かし付き電子サインデータが埋め込まれた商取引情報、つまり、電子透かし付き電子サインデータが得られた場合に与えられるものとする。

【００４４】

次に、電子サイン管理サーバ１００の構成要素を簡単に説明する。

【００４５】

データ送受信部１１０は、業者端末１０との間でデータの送受信を行う部分で、通信インタフェースを備えている。

【００４６】

なお、任意の構成として利用者認証部を備えても良い。利用者認証部は、今回の取引の利用者を真正な利用者であると認証する部分である。サイン照合部１３０から渡されるサインが真正であるか否かの情報に加え、必要に応じて他に入力された暗証番号やバイオメトリック情報、カードの紛失届に関する情報など、利用者の正当性を確認する情報を用いて利用者を認証する。もちろん処理を簡素化し、サインが真正であるか否かの情報のみで利用者が真正であると判断する処理とすることも可能である。

【００４７】

本実施形態１では必須構成として電子透かし付与部１５０を備えている。電子透かし付与部１５０は、業者端末１０から得た商取引情報と手書きサイン入力部

３０から入力された電子サインデータに対して、電子透かし情報を埋め込み、電子透かし付き電子サインデータを生成する部分である。

【００４８】

なお、本実施形態１では任意の構成として商取引管理データ格納部１６０を備えている。商取引管理データ格納部１６０は、電子透かし付与部１５０により生成された電子透かし付き電子サインデータを登録保持しておく部分である。将来、商取引者間において何らかのトラブルが発生した場合に備えて生成した電子透かし付き電子サインデータを登録しておく。

【００４９】

次に、電子透かし付与部１５０の各構成要素を説明する。

【００５０】

電子透かし情報取得部１５１は、電子透かし情報とする情報を取得する部分である。電子透かし情報の一例としては、今回の取引内容を示す商取引識別子、利用者の電子サインデータから生成した要約情報がある。ここで、商取引識別子は、取引内容を個別に特定・識別しうる情報であり、例えば、シリアルに付される番号や暗号のようなものでも良い。さらに、商取引識別子は、少なくとも、該商取引に関わる業者を特定する業者識別情報、該商取引に関わる利用者を特定する利用者識別情報、該商取引を特定するため業者側が付与した商取引業者管理情報、該利用者が入力した電子サインデータ、該商取引に関わる決済金額情報、該商取引の発生した日時情報を含むものであるものでも良い。これら情報は、今回の取引内容を示す商取引を識別するには有効な情報であると考えられるからである。商取引識別子は、業者端末１０から送信され、データ送受信部１１０を介して電子サイン管理サーバ１００に受信される。

【００５１】

本実施形態１では、付加情報として利用者の電子サインデータから生成した要約情報も用いる。要約情報は電子サインデータ要約処理部１５２により生成する。電子サインデータ要約処理部１５２はデータ長要約アルゴリズムに従って、電子サインデータを所定のデータ長となるように圧縮する部分である。電子署名データが改ざんされると、抽出された要約情報と、もう一度計算によって得られる

要約情報に違いが検出されるため、改ざんがあったことが検知できる。

【００５２】

電子透かし付与処理部１５３は、電子サインデータに対して電子透かし情報をを埋め込む処理を実行する部分である。

【００５３】

以下に、電子透かし付与処理部１５３による電子透かし付与処理を詳しく説明する。電子透かしは、電子的なデータの不正コピーを防止することを目的とするもので、電子サインデータに「電子透かし」を埋め込むことにより様々な効果を得ることができる。例えば、人間には外見上「電子透かし」が埋め込まれているかを識別できない。また、電子透かしを埋め込んだ電子サイン管理機関側は必要に応じていつでも透かし情報を読み取ることができる。また、埋め込みアルゴリズムを知らない限り、第三者が電子データから透かし情報を取り除くことはできない。さらに、無理に透かし情報を取り除くと、改ざんがあったことが検知でき、不正なデータであることが判定できる。電子サインデータへの電子透かしの埋め込み方法は複数あり、電子サインデータのデータ形式に応じて使い分けることも可能である。電子サインデータは典型的には２値あるいは他値にビットマップ化された静止画イメージで表現されている場合と二次元の座標点の時系列データとして表現されている場合がある。本実施形態１では、サイン照合をより高精度に実行できる二次元の座標点の時系列データで表現されている場合の電子サインデータに対して電子透かし情報を埋め込む処理を例として説明する。

【００５４】

電子サインデータは、手書きサイン入力部３０を介して取り込まれるが、手書きサイン入力部３０として、電磁誘導式タブレット、感圧式タブレットなど、文字の筆記に伴うペン先の位置と状態の変化を一定時間間隔で検知するデバイスが使われる。このデバイスを使用した場合、図２（ａ）のような電子サインデータは、図２（ｂ）のような、座標点の列のデータとして表現される。正確にいえば、座標点Ｐｉの位置座標をＸｉ，Ｙｉ、その時の属性値をＳｉ＝(PenDown, PenMove, PenUp)とし、座標点ＰｉはＰｉ：（Ｘｉ，Ｙｉ，Ｓｉ）として表現される。そのとき、電子サインデータ全体はＳｉｇｎ＝（ｎ，Ｐ１，Ｐ２，・・，Ｐｎ

）（ｎは自然数であり、座標点数により可変）として表現される。ここでPenDownとは、文字の一画(ストロークと呼ぶ)の第一点、PenUpはストロークの最終点、PenMoveはストロークの途中の点につけられる属性値である。タブレットによっては、属性値として、その時点の筆圧を量子化した情報、筆記開始からの経過間情報、ペンの傾き値情報などの持つ場合もあるし、電子誘導式のようにペンがある程度筆記面から離れていても座標値を検出できる場合には、PenUpがストロークの最終点だけでなく、ペン先が空中を移動している時間にサンプリングした座標点にも付与される場合もある。

【００５５】

電子サインデータに電子透かし情報を埋め込む場合は、人間には検知できない電子データの冗長性部分を利用して行うことが好ましい。電子サインデータの場合、例えば、次のような手法が考えられる。

【００５６】

第１の手法は、位置座標の下位ビットに情報を埋め込む手法である。座標点の位置座標（Ｘｉ，Ｙｉ）を、それぞれ１６ビットで表現したとする。この場合、Ｘ座標，Ｙ座標は縦、横それぞれ６５５３６の解像度を持つことになる。文字をディスプレイ上に表現するには１００×１００ドット程度の解像度があれば十分であり、このような低解像度でも、ＸまたはＹ座標値が±１程度変化しても人間の目には殆ど感知できない。さらに解像度を上げて１６ビット程度で表現してしまえば、下位１～２ビットを電子透かし情報の埋め込みに使っても人間の目に感知することはできず、サイン照合アルゴリズムも、この程度の変化で影響を受けることはない。このような性質を利用してＳｉｇｎ＝（ｎ，Ｐ１，Ｐ２，・・，Ｐｎ）（ｎは自然数であり、座標点数により可変）のうち、電子透かし埋め込みアルゴリズムが定める複数の点Ｐｊ１，Ｐｊ２，・・，Ｐｊｍを選んで、ＸＹ座標値の下位ビットに透かし情報を埋め込む。どの点に埋め込むかは、もちろん非公開であり、それ以外の点に錯乱のためにデータを混入してもよい。

【００５７】

第２の手法は、冗長な座標点を埋め込む手法である。電子サインデータがディスレイやプリンタに表示される時、PenDownからPenUpまでの一連の点列は折れ線

(またはより滑らかにするためスプライン曲線やベジエ曲線)で繋がれて、通常座標点自体が明確に表示されることはない。このため、PenMoveの段階でＰｉと全く同一の点がＰｉの後に挿入されてＳｉｇｎ＝（ｎ＋１，Ｐ１，Ｐ２，・・，Ｐｉ，Ｐｉ，・・，Ｐｎ）（ｎは可変）となっても、人間の目に知覚できない。このように同じ位置座標を持つ点を連続して埋め込むことによって透かし情報を埋め込むことが可能である。

【００５８】

第３の手法は、冗長な座標点を埋め込む手法で上記第２の手法と異なるものである。第２の手法は、全く同じ座標点が連続することになるので、同じ座標点が連続しているか否かを探知することにより、どれが電子透かし情報の座標点であるか見破られやすい。そこで、まったく同じ座標値を埋め込むのではなく、図３のように連続する二つの座標点Ｐｉ，Ｐｉ＋１の間に、ＰｉとＰｉ＋１をＮ：Ｍに内分する座標点Ｐｉ’を埋め込む。この場合、座標点Ｐｉ’が埋め込まれてもやはり人間に変化を感知することはできない。また、この場合は何対何に内分するかという自由度があり、これによって電子透かし情報の埋め込みにおいて複数の選択冗長が得られ、どの点が埋め込まれた座標点であるか容易には検知できないため安全性が高くなる。例えば、Ｎ：Ｍが１：１，１：２，１：３，１：４のいずれかとすれば座標点の埋め込み１点あたり２ビット分の冗長性が得られ、４通りの埋め込めみが可能となる。どの位置Ｐｉに埋め込むかは、当然非公開とする。

【００５９】

以上、電子サインデータへの電子透かし情報の埋め込み手法を説明したが、本発明の電子商取引システムおよび方法において、上記埋め込み手法以外も用いることができ、また、同時に複数の手法を組み合わせてより埋め込み情報量を増やしたり、安全性を高めることも可能である。

【００６０】

埋め込みアルゴリズムを秘密にすれば、第三者に埋め込んだ情報を読み取られる危険性は少ないが、これだけでは電子サインデータの改ざんを防止できない。そのため本発明の電子商取引システムおよび方法では改ざん防止手法として、電

子サインデータ要約処理部１５２により電子サインデータ全体に対して要約関数を適用し、所定ビットの要約情報を生成する。要約情報のビット量としては、８ビット程度でも実用上十分である。この要約情報を付加情報として電子透かし情報取得部１５１に渡し、電子透かしデータの一部として用い、Ｎビットの要約情報を電子透かしとして埋め込む。電子署名データが改ざんされると、抽出された要約情報と、もう一度計算によって得られる要約情報に違いが検出されるため、改ざんがあったことが検知できる。

【００６１】

電子透かし付与部１５０は、上記のように電子サインデータに対して電子透かし情報を埋め込み、電子透かし付き電子サインデータを生成する。さらに、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部１６０に登録保持しておくことが好ましい。

【００６２】

本実施形態１の構成は利用者確認部１５４を備えている。利用者確認部１５４は、登録されている利用者の連絡先データを基に利用者に対して直接、該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う部分である。業者側の偽サインの流用による架空の取引を防止するためのセキュリティ向上手段の一つである。取引を成立させる前に利用者に対して確認をとるもので、業者端末１０を介さずに、利用者確認部１５４と利用者がネットワーク３００などの通信路を介して直接通信し合うことが好ましい。

【００６３】

例えば、利用者の連絡先データとして携帯電話の番号を保持し、利用者の携帯電話を利用して利用者確認部１５４と利用者が電話回線を介して確認内容の問い合わせをする。この場合、利用者確認部１５４が電話通信手段と音声応答システムを備え、利用者の携帯電話などの携帯端末４００を介して利用者への確認内容を音声情報により問い合わせ、利用者確認を得ることも可能である。一例として、コンピュータの音声合成により「取引を承認する場合は「１」のボタン、承認しない場合は「０」のボタンを押して下さい」とのメッセージを発生し、「登録判定プログラム」は利用者のボタン操作によって登録確認の可否を判断する。ま

た、他の例としては、利用者確認部１５４が、利用者が保持する携帯端末４００との通信手段を備え、携帯端末４００を介して利用者への確認内容を電子データとして問い合わせ、電子データにより確認を得る。利用者端末がマルチメディア電子メール等を受信できる装置であれば、「利用者認証機関」は例えばジャバスクリプトにより記述された返信応答ボタンが付与されたＨＴＭＬ表現の電子メールを利用者端末に送付し、画面上に「○○の取引を承認する場合には、「ＹＥＳ」ボタン、承認しない場合は「ＮＯ」ボタンを押して下さい」という案内で確認操作の指示をすることもできる。また、音声認識部を備え、音声で「はい」とか「いいえ」で答えるようにしても良い。

【００６４】

利用者確認部１５４は、利用者からの確認が得られない場合は、電子透かし付き電子サインデータの生成を拒否することとし、業者端末の制御部４０に対して拒否の旨を通知する。

【００６５】

このように業者端末１０を介さずに利用者確認部１５４と利用者が直接通信し合うことで架空の取引を取引成立前に事前に察知することができ、電子商取引システムのセキュリティを向上することが可能となる。

【００６６】

次に、本実施形態１の電子商取引システムおよび方法の動作の流れを図４のフローチャートを参照しつつ説明する。

【００６７】

まず、利用者と業者の間で商品購入など取引内容が定められる。業者は、業者コード、業者が個々の取引を識別するために付与する取引コード、取引金額など取引内容に関する情報を取引内容入力部１１を介して業者端末１０に入力し、一方、利用者は利用者識別情報を利用者識別情報読み取り部２０を介して業者端末１０に入力する（ステップＳ４０１）。なお、カード媒体から利用者識別情報を読み取る場合は、業者が利用者に代わってカードを利用者識別情報読み取り部２０であるカードリーダに挿入して読み取られせることも可能である。バイオメトリック情報である場合などは利用者自らが利用者識別情報読み取り部２０を操作

する。

【００６８】

業者端末の制御部４０は、取引内容に関する情報と利用者識別情報を決済機関のサーバ２００に送る。決済機関のサーバ２００はカードの有効性や利用者に対する信用枠、業者が加盟業者であるかなどを確認し、商取引情報生成部２１０により商取引情報を生成する（ステップＳ４０２）。なお、決済機関のサーバ２００と業者端末１０とは専用回線あるいはインターネット、無線通信回線などの電子データを相互に送受信できるネットワーク３００にて結ばれているものとする。

【００６９】

生成された商取引情報は決済機関のサーバ２００から商取引情報提示部３１に渡され、商取引情報提示部３１は商取引情報を利用者に提示する（ステップＳ４０３）。

【００７０】

利用者は、提示された商取引情報から取引内容を確認し（ステップＳ４０４）、取引に同意する場合（ステップＳ４０４：Ｙ）、手書きサイン入力部３０を介して手書きサイン欄にサインを手書き入力する（ステップＳ４０５）。

【００７１】

手書きサイン入力部３０は、手書き入力されたサインから、最終的な筆跡形状、書き順、筆圧、筆記速度など照合処理に用いる情報を電子化した電子サインデータを得て、電子サインデータと商取引情報を電子サイン管理サーバ１００に送信する（ステップＳ４０６）。なお、電子サイン管理サーバ１００と業者端末１０とは専用回線あるいはインターネット、無線通信回線などの電子データを相互に送受信できるネットワーク３００にて結ばれているものとする。

【００７２】

次に、電子サイン管理サーバ１００は、データ送受信部１１０を介して電子サインデータと商取引情報を受け取る。なお、ここで、他の暗証番号やバイオメトリック情報、カードの紛失届に関する情報など、利用者の正当性を確認する情報がある場合には当該情報用いて利用者をチェックすることもできる。

【００７３】

本実施形態１の構成では、利用者確認部１５４により、利用者に対して直接、電子透かし付き電子サインデータ生成を実行しても良いか確認する（ステップＳ４０７）。つまり、利用者の保持する携帯電話や携帯端末を介して音声案内や電子データにより本人に対して該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う。

【００７４】

利用者からの確認が得られれば（ステップＳ４０７：Ｙ）、電子透かし付与部１５０による処理が開始する。本実施形態１の構成では、電子サインデータ要約処理部１５２により電子サインデータから要約情報を生成し（ステップＳ４０８）、電子透かし情報取得部１５１が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップＳ４０９）、電子透かし付与処理部１５３が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップＳ４１０）。

【００７５】

なお、電子サイン管理サーバ１００は、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部１６０に登録する。さらに、電子サイン管理サーバ１００はデータ送受信部１１０を介して、生成した電子透かし付き電子サインデータを業者端末１０に送信し、商取引データ格納部５０に格納する（ステップＳ４１１）。

【００７６】

なお、この電子透かし付き電子サインデータは、業者端末１０からまたは電子サイン管理サーバ１００から決済機関のサーバ２００に対して送信され、決済機関により該商取引に対する信用保証が与えられる。

【００７７】

なお、上記ステップＳ４０４において取引に同意しない場合（ステップＳ４０４：Ｎ）、上記ステップＳ４０７において利用者からの確認が得られなかった場合（ステップＳ４０７：Ｎ）は、いずれも、今回の商取引に対する信用保証を与

えることができないとして、電子商取引処理を終了する。

【００７８】

以上が、本実施形態１の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【００７９】

なお、決済機関における処理として、商取引情報を電子透かしとして電子透かし付き電子サインデータを生成し、該情報を決済機関側でも格納しておき、決済時に決済機関側において、業者端末側が送ってきた電子透かし付き電子サインデータと照合するという決済手順も可能である。

【００８０】

上記構成による電子商取引システムおよび方法とすることにより、業者は電子透かし付き手書き電子署名データを複製したり、他の架空取引に流用するような行為を行うことはできない。実際にそのような行為が行われれば、架空取引に関する電子透かし付き電子サインデータを基に、電子サイン管理機関に対して、商取引管理データ格納部１６０に登録された電子透かし付き電子サインを検索し、正式に商取引として登録されたものであるか、正式に登録されたものであれば、いつ、なんの取引の時に使用した電子サインであるかを知ることができるからである。

【００８１】

また、応用的な運用として、電子サイン管理機関は、利用者認証時に利用者に直接確認を行うことにより、業者、あるいは、第三者によって、利用者が認知しない架空のサイン登録が電子サイン管理機関に行われることを防ぐことができる。この応用的な運用を行う場合、利用者が携帯端末を該商取引実行時に保持している必要性があるが、近年の携帯電話やｉモードの普及率を見れば、このような運用も十分期待できる。また、当該確認は、取引時にリアルタイムに実施しなくても、例えば、一日以内、あるいは一週間以内に行い、その段階で利用者承認が得られなければ商取引の取り消し（無効）を実施するというものでも良い。この場合には、利用者確認部は、有線電話通信、ＦＡＸ通信、電子メール通信、手紙

等任意の手段であっても良い。

【００８２】

（実施形態２）

実施形態２の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。

【００８３】

図５は、実施形態２の電子商取引システムの構成例を示すブロック図である。

【００８４】

図５において、電子サイン管理サーバ１００ａ、決済機関のサーバ２００ａ、ネットワーク３００の諸構成要素は実施形態１で説明した図１と同様であるが、業者端末１０ａは利用者識別情報読み取り部２０、業者端末の制御部４０、商取引データ格納部５０、データ送受信部６０を備えているが、手書きサイン入力部３０および商取引情報提示部３１が設けられておらず、利用者の携帯端末４００ａが手書きサイン入力部３０および商取引情報提示部３１を備えた構成となっている。なお、各要素は実施形態１と同様であるのでここでの説明は省略する。

【００８５】

図５の構成によれば、手書きサイン入力部３０が業者端末１０に接続されていないので、利用者が保持する携帯端末４００ａを介して利用者と電子サイン管理サーバ１００ａが直接データ通信し合うことにより電子サインデータがやりとりでき、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティ強度がさらに向上する。

【００８６】

図５の構成の場合、決済機関のサーバ２００ａの商取引情報生成部２１０が生成した商取引情報が直接、利用者の携帯端末４００ａに送信され、商取引情報提示部３１に提示されることとなる。利用者は商取引情報の内容を確認し、手書きサイン入力部３０に対して手書きサインを書き込む。利用者の携帯端末４００ａは、商取引情報と電子サインデータを電子サイン管理サーバ１００ａに対して直接送信する。電子サイン管理サーバ１００ａにおいて電子透かしが付され、業者端末１０に対しては、電子透かし付き電子サインデータという形で渡されること

となり、実施形態１のように、電子透かしが未だ付されていない状態の電子サインデータが業者端末１０ａを経由することはない。それゆえ、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティがさらに向上する。さらに、利用者は業者端末１０ａに接続された手書きサイン入力部３０に対して入力する必要がないので、プライバシー保護が向上し、心理的効果として安心して電子商取引を行うことができる。

【００８７】

本実施形態２の電子商取引システムおよび方法の動作の流れを図６のフローチャートを参照しつつ説明する。

【００８８】

まず、取引内容入力部１１および利用者識別情報読み取り部２０を介した取引内容に関する情報および利用者識別情報の入力処理（ステップＳ６０１）、決済機関のサーバ２００ａの商取引情報生成部２１０による商取引情報の生成（ステップＳ６０２）は実施形態１に示した図４のフローチャートに示したステップＳ４０１とステップＳ４０２の処理と同様である。

【００８９】

次に、決済機関のサーバ２００ａは、生成した商取引情報を、無線電話回線などのネットワーク３００を通じて、利用者が保持する携帯電話などの携帯端末４００ａに対して直接送信し、携帯端末４００ａの商取引情報提示部３１は受信した商取引情報を利用者に提示する（ステップＳ６０３）。

【００９０】

利用者は、提示された商取引情報から取引内容を確認し（ステップＳ６０４）、取引に同意する場合（ステップＳ６０４：Ｙ）、利用者端末４００ａが備える手書きサイン入力部３０を介して手書きサイン欄にサインを手書き入力する（ステップＳ６０５）。

【００９１】

手書きサイン入力部３０は手書き入力したサインから電子サインデータを生成し、携帯端末４００ａから無線電話回線などのネットワーク３００を通じて、電子サイン管理サーバ１００ａに対して直接送信する（ステップＳ６０６）。なお

、商取引情報は、利用者端末４００ａが電子サインデータとともに電子サイン管理サーバ１００ａに対して送信しても良く、また、決済機関のサーバ２００ａから電子サイン管理サーバ１００ａに対して送信しても良い。

【００９２】

なお、電子サイン管理サーバ１００ａにおける処理、つまり、利用者確認部１５４による利用者に対する利用者認証是非の利用者確認処理（ステップＳ６０７）、電子サインデータ要約処理部１５２による電子サインデータからの要約情報の生成（ステップＳ６０８）、電子透かし情報取得部１５１による付加情報の取得（ステップＳ６０９）、電子透かし付与処理部１５３による電子透かし付き電子サインデータの生成処理（ステップＳ６１０）に関しては、実施形態１の図４のフローチャートの処理と同様で良い。

【００９３】

最後に、電子サイン管理サーバ１００ａは、商取引における何らかのトラブルに備えるべく、電子透かし付き電子サインを商取引管理データ格納部１６０に登録し、さらに、電子サイン管理サーバ１００ａはデータ送受信部１１０を介して、生成した電子透かし付き電子サインデータを業者端末１０ａに送信し、商取引データ格納部５０に格納する（ステップＳ６１１）。

【００９４】

以上が、本実施形態２の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【００９５】

上記構成による電子商取引システムおよび方法とすることにより、利用者が保持する携帯端末４００ａを用いて電子サイン管理サーバ１００ａに対して直接電子サインデータを送信することができ、悪意の業者によるサインの盗用や複製といった不正行為に対するセキュリティ強度がさらに向上する。

【００９６】

（実施形態３）

実施形態３の電子商取引システムおよび電子商取引方法を図を参照しつつ説明

する。本実施形態３は、電子透かし付与部を第３者機関に設けた構成ではなく、利用者端末に設ける構成としたものである。

【００９７】

図７は、実施形態３の電子商取引システムの構成例を示すブロック図である。

【００９８】

図７において、決済機関のサーバ２００ｂ、ネットワーク３００の諸構成要素は実施形態１で説明した図１と同様であるが、電子サイン管理サーバ１００に相当する部分は設けられていない構成となっている。業者端末１０ｂは利用者識別情報読み取り部２０、業者端末の制御部４０、商取引データ格納部５０、データ送受信部６０を備えている。利用者の携帯端末４００ｂは、手書きサイン入力部３０および商取引情報提示部３１に加え、電子透かし付与部１５０と電子透かし付き電子サインデータ格納部１６０を備えた構成となっている。なお、各要素は実施形態１と同様であるのでここでの説明は省略する。

【００９９】

図７の構成によれば、電子透かし付与部１５０が利用者端末４００ｂに設けられているので、実施形態１や実施形態２の構成により必要となる電子透かし付与処理に対する利用者確認を不要とすることができ、また、電子サイン管理サーバとのやり取りも不要となる。さらに、電子透かし付加処理は利用者端末４００ｂにおいて行うので、実施形態１、実施形態２のように電子透かし付加処理前の利用者の確認を行う必要もなくなる。

【０１００】

本実施形態３の電子商取引システムおよび方法の動作の流れを図８のフローチャートを参照しつつ説明する。

【０１０１】

まず、取引内容入力部１１および利用者識別情報読み取り部２０を介した取引内容に関する情報および利用者識別情報の入力処理（ステップＳ８０１）、決済機関のサーバ２００ｂの商取引情報生成部２１０による商取引情報の生成（ステップＳ８０２）、携帯端末４００ｂの商取引情報提示部３１を介した商取引情報の利用者への提示（ステップＳ８０３）、提示された商取引情報に対する利用者

による確認の是非（ステップＳ８０４）、利用者端末４００ｂが備える手書きサイン入力部３０を介した手書きサインの入力（ステップＳ８０５）、手書きサイン入力部３０から生成された電子サインデータの電子サイン管理サーバ１００ｂへの送信（ステップＳ８０６）は実施形態２に示した図６のフローチャートに示したステップＳ６０１とステップＳ６０６の処理と同様である。なお、本実施形態３では、ステップＳ６０７の利用者確認部１５４による利用者確認処理は実行されない。

【０１０２】

次に、利用者端末４００ｂは、電子サインデータ要約処理部１５２により電子サインデータから要約情報を生成し（ステップＳ８０７）、電子透かし情報取得部１５１が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップＳ８０８）、電子透かし付与処理部１５３が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップＳ８０９）。

【０１０３】

利用者端末４００ｂは、生成した電子透かし付き電子サインデータを業者端末１０ｂに送信し、商取引データ格納部５０に格納する（ステップＳ８１０）。

【０１０４】

以上が、本実施形態３の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【０１０５】

上記構成による電子商取引システムおよび方法とすることにより、電子透かし付与部が利用者端末に設けられているので、電子透かし付与処理に対する利用者確認を不要とすることができる。

【０１０６】

（実施形態４）

実施形態４の電子商取引システムおよび電子商取引方法を図を参照しつつ説明する。本実施形態４は、サイン認証部１７０を追加した構成としたものである。

【０１０７】

図９は、実施形態４の電子商取引システムの構成例を示すブロック図である。

【０１０８】

図９において、業者端末１０ｃ、決済機関のサーバ２００ｃ、ネットワーク３００、利用者の携帯端末４００ｃの諸構成要素は実施形態１で説明した図１と同様であるが、電子サイン管理サーバ１００ｃは、サイン認証部１７０を備えている構成となっている。なお、サイン認証部１７０以外の各要素は実施形態１と同様であるのでここでの説明は省略する。

【０１０９】

サイン認証部１７０は、利用者から入力された手書きサインが真正のサインであるか否かを認証する部分である。サイン認証部１７０は以下の構成要素を備えている。

【０１１０】

登録サイン格納部１７１は、あらかじめ利用者がクレジットカード生成時などに提供した利用者の真正サインを登録電子サインデータとして格納しておく部分である。ここでは実施形態１で説明した場合と同様、電子データとして登録保持されるものとする。

【０１１１】

サイン照合部１７２は、登録サイン格納部１７１に格納されている登録電子サインデータと、手書きサイン入力部３０から入力された利用者の電子サインデータをマッチングし、照合処理する部分である。システムに要求される照合精度に応じて、最終的な筆跡形状のみならず、利用者の書き順、筆圧、筆記速度など多様な情報を用いて照合処理を行い、入力されたサインが真正であるか否かの情報を出力する。

【０１１２】

このサイン認証部１７０を設けた構成によれば、登録されている真正の電子サインデータと、商取引において手書きサイン入力部３０から入力された利用者の電子サインデータをマッチングすることができ、利用者認証を高いセキュリティレベルで行うことができる。従来は業者自身が店頭において今回手書きされたサ

インと利用者カードの裏面などに書かれたサインとを目視により照合していたが、より正確かつ高いセキュリティによりサインの照合を行うことができる。

【０１１３】

本実施形態４の電子商取引システムおよび方法の動作の流れを図１０のフローチャートを参照しつつ説明する。

【０１１４】

まず、取引内容入力部１１および利用者識別情報読み取り部２０を介した取引内容に関する情報および利用者識別情報の入力処理（ステップＳ１００１）、決済機関のサーバ２００ｃの商取引情報生成部２１０による商取引情報の生成（ステップＳ１００２）、携帯端末４００ｃの商取引情報提示部３１を介した商取引情報の利用者への提示（ステップＳ１００３）、提示された商取引情報に対する利用者による確認の是非（ステップＳ１００４）、利用者端末４００ｃが備える手書きサイン入力部３０を介した手書きサインの入力（ステップＳ１００５）、手書きサイン入力部３０から生成された電子サインデータの電子サイン管理サーバ１００ｃへの送信（ステップＳ１００６）は実施形態２に示した図６のフローチャートに示したステップＳ６０１とステップＳ６０６の処理と同様である。

【０１１５】

本実施形態４の電子商取引システムおよび方法では、サイン認証処理を実行する。電子サイン管理サーバ１００ｃは、データ送受信部１１０を介して電子サインデータと商取引情報を受け取り、商取引情報の利用者識別情報から登録サイン格納部１７１に格納されている利用者の登録サインデータを検索し、サイン照合部１７２において登録電子サインデータと利用者の電子サインデータをマッチングし、照合処理する（ステップＳ１００７）。

【０１１６】

次に、利用者確認部１５４により、利用者に対して直接、利用者認証しても良いか確認する（ステップＳ１００８）。つまり、該商取引における電子透かし付き電子サインデータ生成の是非の確認を行う。

【０１１７】

利用者からの確認が得られれば（ステップＳ１００８：Ｙ）、電子透かし付加

処理に移行する。電子サイン管理サーバ１００ｃは、電子サインデータ要約処理部１５２により電子サインデータから要約情報を生成し（ステップＳ１００９）、電子透かし情報取得部１５１が今回の取引内容を特定する商取引識別子や要約情報などを電子透かし情報として取得し（ステップＳ１０１０）、電子透かし付与処理部１５３が非公開のアルゴリズムにより電子サインデータに対して電子透かしとして埋め込み、電子透かし付き電子サインデータを生成する（ステップＳ１０１１）。

【０１１８】

電子サイン管理サーバ１００ｃは、生成した電子透かし付き電子サインデータを業者端末１０ｃに送信し、商取引データ格納部５０に格納する（ステップＳ１０１２）。

【０１１９】

以上が、本実施形態４の電子商取引システムおよび方法の処理の流れである。もちろん、上記処理の流れは一例であり、本発明の技術思想の及ぶ範囲において他の処理の流れとすることも可能である。

【０１２０】

以上、本実施形態４の電子商取引システムおよび方法によれば、電子サイン管理サーバ１００ｃによる利用者認証を行う処理が実行されないので、商取引の処理内容を低減することができ、処理の効率化を図ることができる。

【０１２１】

（実施形態５）

本実施形態５の電子商取引システムおよび方法は、実運用上の使い勝手を向上する工夫を加えたものである。現在、一部のクレジットカードの運用や、一部のデビッドカードの運用において、一定額以下の小額取引については、店舗内での手続時間の短縮化や、利用者の手続負担軽減のため、取引伝票に対するサインを省略するという運用が見られる。本実施形態５の電子商取引システムおよび方法は、一定額以下の小額取引などについては手書きサイン入力を省略し、電子透かし付き電子サインデータの生成に代え、電子透かし付き電子サイン省略商取引情報を生成して決済を完了するものである。

【０１２２】

図１１は、実施形態５の電子商取引システムの構成例を示すブロック図である。図１１において、決済機関のサーバ２００ｄは、手書きサイン省略可否判定部２２０を備えている。手書きサイン省略可否判定部２２０は、業者識別情報、利用者識別情報、決済金額情報など商取引情報に基づいて、手書きサインによる利用者認証処理を省略するか否かを判断する部分である。例えば、業者識別情報に基づいて業者の別に応じてサインを省略する運用を認めるか否かを調整したり、利用者識別情報に基づいて利用者の別に応じてサインを省略する運用を認めるか否かを調整したり、さらに、決済金額情報に基づいて、決済金額の大きさに応じてサインを省略する運用を認めるか否かを調整することができる。手書きサイン省略可否判定部２２０により手書きサインの省略が認められた場合、手書きサイン入力部３０による電子サインデータ読み取りと、電子透かし付与部１５０による電子透かし付き電子サインデータの生成が省略され、商取引データ格納部５０に利用者識別情報と商取引情報を格納するものである。

【０１２３】

なお、図１１のその他の構成要素は実施形態１の図１や実施形態２の図５のものと同様で良い。ここでは決済機関のサーバ２００ｄ以外の構成は図１のものと同様の例とする。なお、ここでのその他の各要素の説明は省略する。

【０１２４】

図１２は、実施形態５の電子商取引システムおよび方法の処理の流れの例を示すフローチャートである。

【０１２５】

まず、取引内容入力部１１および利用者識別情報読み取り部２０を介した取引内容に関する情報および利用者識別情報の入力処理（ステップＳ１２０１）、決済機関のサーバ２００ｄの商取引情報生成部２１０による商取引情報の生成（ステップＳ１２０２）は実施形態１に示した図４のフローチャートに示したステップＳ４０１とステップＳ４０２の処理と同様である。

【０１２６】

次に、決済機関のサーバ２００ｄは、手書きサイン省略可否判定部２２０によ

り、業者識別情報、利用者識別情報、決済金額情報など商取引情報に基づいて手書きサインによる利用者認証処理を省略するか否かを判定する（ステップＳ１２０３）。

【０１２７】

手書きサインによる利用者認証処理を省略する場合（ステップＳ１２０３：Ｙ）、実施形態１において実行されるステップＳ４０４～ステップＳ４１１、または、実施形態２において実行されるステップＳ６０４～ステップＳ６１１、または、実施形態３において実行されるステップＳ８０４～ステップＳ８１０、または、実施形態４において実行されるステップＳ１００４～ステップＳ１０１２までの処理が省略され、電子透かし付与部１５０は、商取引情報に対して、電子透かし付き電子サインの埋め込みを省略し（ステップＳ１２０４）、商取引データ格納部５０に利用者識別情報と商取引情報を格納する。（ステップＳ１２０５）。

【０１２８】

以上、本実施形態５による電子商取引システムおよび方法は、一定額以下の小額取引などについては手書きサイン入力を省略して決済を完了することができ、店舗内での手続時間の短縮化や、利用者の手続負担軽減を図ることができる。

【０１２９】

（実施形態６）

実施形態６の電子商取引システムおよび方法は、事後的に商取引における何らかのトラブルにより、電子サインの正当性が問題となった場合に、電子サインが正当なものであるか不正なものかを確認する処理を実行するものである。

【０１３０】

図１３が本実施形態６の電子サインの正当性を確認するためのシステム構成例を示すブロック図である。９００が電子サイン検証装置である。電子サイン検証装置９００は、商取引情報取得部９１０、電子透かし付き電子サインデータ取得部９２０、改ざんチェック部９３０、商取引識別子抽出部９４０、商取引情報検索部９５０、商取引情報格納部９５１、検証部９６０を備えている。

【０１３１】

商取引情報取得部９１０および電子透かし付き電子サインデータ取得部９２０は、検証すべき商取引の結果として保存されている商取引情報および電子透かし付き電子サインデータを取得する部分である。取得された商取引情報は検証部９６０に渡され、電子透かし付き電子サインデータは後述する処理実行のため改ざんチェック部９３０に渡される。

【０１３２】

改ざんチェック部９３０は、商取引に用いられた電子サインデータに改ざんがないかをチェックする部分である。改ざんチェック部９３０は電子サインデータに埋め込まれている電子透かし情報を調べることにより電子サインデータの改ざんの有無を判定する。この実施形態６では特に電子サインの要約情報を調べることにより電子サインデータの改ざんの有無を判別するものとする。電子サインデータに対して何らかの改ざんを行った場合、付されている要約情報と対応しなくなってしまうので改ざんの有無を判別することが可能となる。つまり、電子サイン自体が不正に書き換えられている場合は、要約情報が異なるものとなり、改ざんチェック部において電子サインデータへの不正行為が検証できるわけである。改ざんチェック部９３０は、改ざんを検出した場合は検証部９６０に送り、検証部９６０は不正検証結果を出力する。改ざんチェック部９３０が改ざんを検出しない場合は、商取引識別子抽出部９４０へ電子透かし付き電子サインデータを渡す。

【０１３３】

商取引識別子抽出部９４０は、電子透かし付き電子サインデータから商取引識別子を抽出する部分である。

【０１３４】

商取引情報検索部９５０は、商取引識別子抽出部９４０が抽出した商取引識別子を検索キーとして商取引情報格納部９５１に格納されている商取引情報を検索する部分である。なお、商取引情報格納部９５１は、事前に電子サイン検証装置９００に用意されている真正取引情報が蓄積されたデータベースであり、例えば商取引時に電子サイン管理サーバなどに格納された商取引情報を取り寄せて該真正の商取引情報を格納したデータベースである。実施形態１などで示した電子サ

イン管理サーバ１００では商取引管理データ格納部１６０において格納された商取引情報に相当するデータベースであれば良い。なお、この実施形態６および図１３のシステム構成例においては電子サインの正当性を確認するシステム９００が商取引情報格納部９５１を含んだ構成としているが、商取引情報格納部９５１に相当するものをシステム９００内に持たず、決済機関など第三者機関が格納しているデータベースを利用する構成であっても良い。

【０１３５】

検証部９６０は、商取引情報取得部９１０から入力された商取引情報、つまり、検証すべき商取引情報と、商取引情報検索部９５０により検索された商取引情報、つまり、電子透かし付き電子サインデータから抽出した当該電子サインに対応する商取引情報の両者を比較・照合する部分である。この両者の比較・照合において両者が一致すれば当該電子透かし付き電子サインデータは真正のもので対応する商取引情報に対して正当なものであったことが検証され、両者が一致しない場合は、逆に当該電子透かし付き電子サインデータは対応する商取引情報に対して正当なものではないことが検証される。つまり、電子サイン自体は過去に正当に利用者により書き込まれたものであるが、他の架空取引に不正に流用されたものであるので対応する商取引情報が異なるものとなる。

【０１３６】

本実施形態６の電子商取引システムおよび方法によれば、電子サイン偽造、電子サイン流用いずれの不正に対してもその正当性を検証することができる。

【０１３７】

（実施形態７）

本発明の電子透かし付き電子サインを用いた電子商取引システムは、上記に説明した構成を実現する処理ステップを記述したプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することにより、各種コンピュータを用いて構築することができる。本発明の電子透かし付き電子サインを用いた電子商取引システムを実現する処理ステップを備えたプログラムを記録した記録媒体は、図１４に図示した記録媒体の例に示すように、ＣＤ－ＲＯＭ１００２やフレキシブルディスク１００３等の可搬型記録媒体１００１だけでなく、ネットワーク上にあ

る記録装置内の記録媒体１０００や、コンピュータのハードディスクやＲＡＭ等の記録媒体１００５のいずれであっても良く、プログラム実行時には、プログラムはコンピュータ１００４上にローディングされ、主メモリ上で実行される。

【０１３８】

【発明の効果】

本発明の電子透かし付き電子サインを用いた電子商取引システムによれば、本発明によれば、電子サインの利用により業者側あるいは第三者の悪意による電子サインの不正利用を防止できるため、カード取引によるサイン入力の電子化が可能となり、それによって利用者側の不正カード利用の防止や紙の取引伝票の保管コストなどの経費削減に効果がある。

【０１３９】

また、利用者が保持する携帯端末に手書きサイン入力部を設ける構成として業者側の悪意による不正利用に対するセキュリティを高めることができる。

【０１４０】

また、電子透かし付与を利用者端末側で実行して、処理ステップを低減し、処理効率を向上することができる。

【０１４１】

また、電子透かし情報として、利用者識別情報や商取引情報などに加え、電子サインデータから生成した要約情報を用いることができ、改ざんの困難な電子透かし情報を用いることができる。

【図面の簡単な説明】

【図１】　本発明の実施形態１の電子商取引システムの構成例を示すブロック図

【図２】　（ａ）は電子サインの筆跡形状の例を示す図、（ｂ）は座標点の列のデータとして表現された電子サインデータの例を示す図

【図３】　連続する二つの座標点Ｐｉ，Ｐｉ＋１の間に、ＰｉとＰｉ＋１をＮ：Ｍに内分する座標点Ｐｉ’が埋め込まれる様子を模式的に表した図

【図４】　実施形態１の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図５】　本発明の実施形態２の電子商取引システムの構成例を示すブロック図

【図６】　実施形態２の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図７】　本発明の実施形態３の電子商取引システムの構成例を示すブロック図

【図８】　実施形態３の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図９】　本発明の実施形態４の電子商取引システムの構成例を示すブロック図

【図１０】　実施形態４の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図１１】　本発明の実施形態５の電子商取引システムの構成例を示すブロック図

【図１２】　実施形態５の電子商取引システムおよび方法の動作の流れの例を示すフローチャート

【図１３】　本実施形態６の電子サインの正当性を確認するためのシステム構成例を示すブロック図

【図１４】　本発明の実施形態６の電子透かし付き電子サインを用いた電子商取引システムを実現する処理プログラムを格納した記録媒体の例を示す図

【図１５】　従来の電子商取引方法を組み合わせたシステム構築例を示す図

【符号の説明】

１０，１０ａ，１０ｂ，１０ｃ，１０ｄ　業者端末

１１　取引内容入力部

２０　利用者識別情報読み取り部

３０　手書きサイン入力部

３１　商取引情報提示部

４０　制御部

５０　商取引データ格納部

６０，１１０　データ送受信部

１００，１００ａ，１００ｂ，１００ｃ　電子サイン管理サーバ

１４０　利用者認証部

１５０　電子透かし付与部

１５１　電子透かし情報取得部

１５２　電子サインデータ要約処理部

１５３　電子透かし付与処理部

１５４　利用者確認部

１６０　商取引管理データ格納部

１７０　サイン認証部

１７１　登録サイン格納部

１７２　サイン照合部

２００，２００ａ，２００ｂ，２００ｃ，２００ｄ　決済機関のサーバ

２１０　商取引情報生成部

２２０　手書きサイン省略可否判定部

３００　ネットワーク

４００，４００ａ，４００ｂ，４００ｃ　利用者の携帯端末

９００　電子サイン検証装置

９１０　商取引情報取得部

９２０　電子透かし付き電子サインデータ取得部

９３０　改ざんチェック部

９４０　商取引識別子抽出部

９５０　商取引情報検索部

９５１　商取引情報格納部

９６０　検証部

１０００　記録装置内の記録媒体

１００１　可搬型記録媒体

１００２　ＣＤ－ＲＯＭ

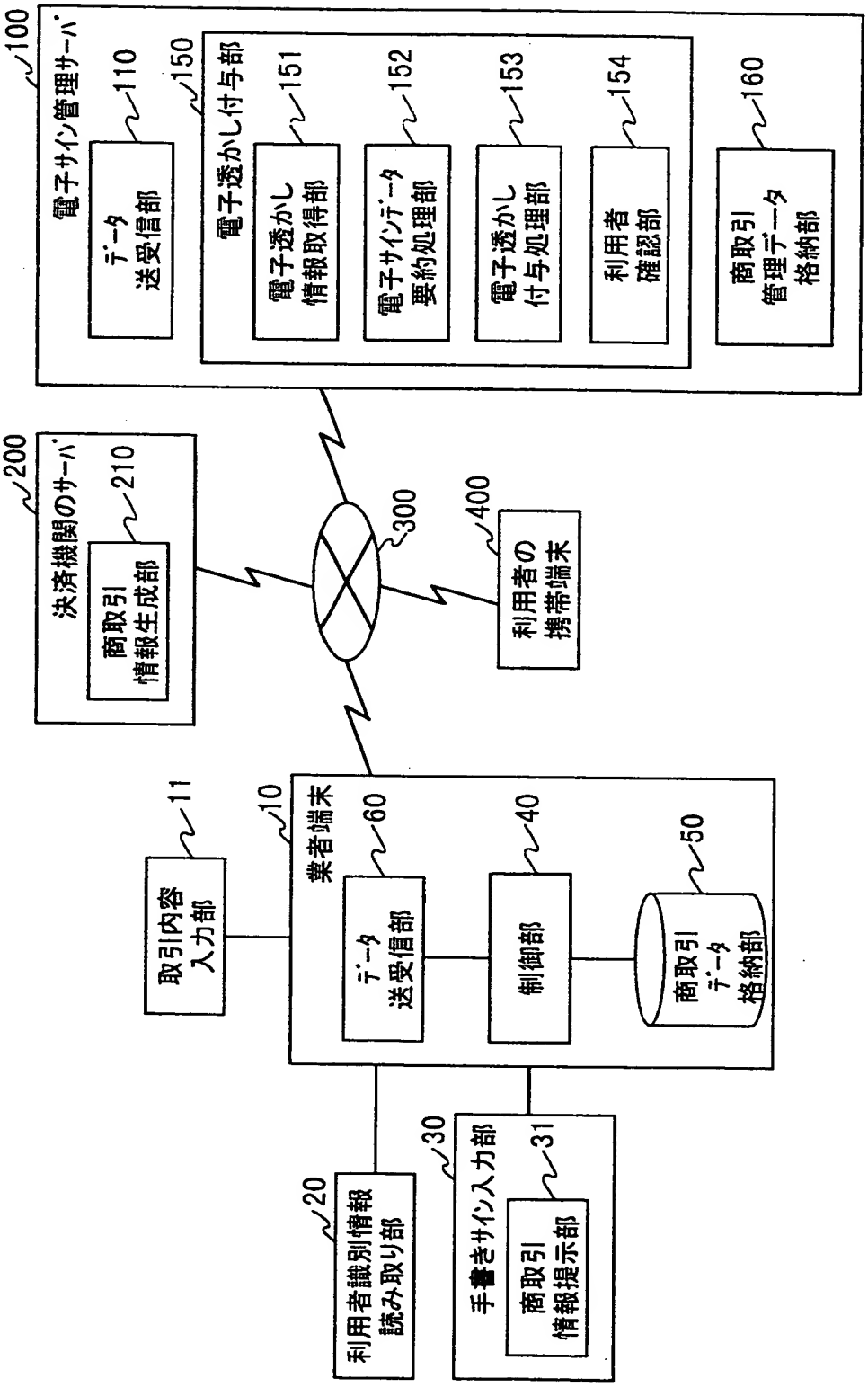
１００３　フレキシブルディスク

１００４　コンピュータ

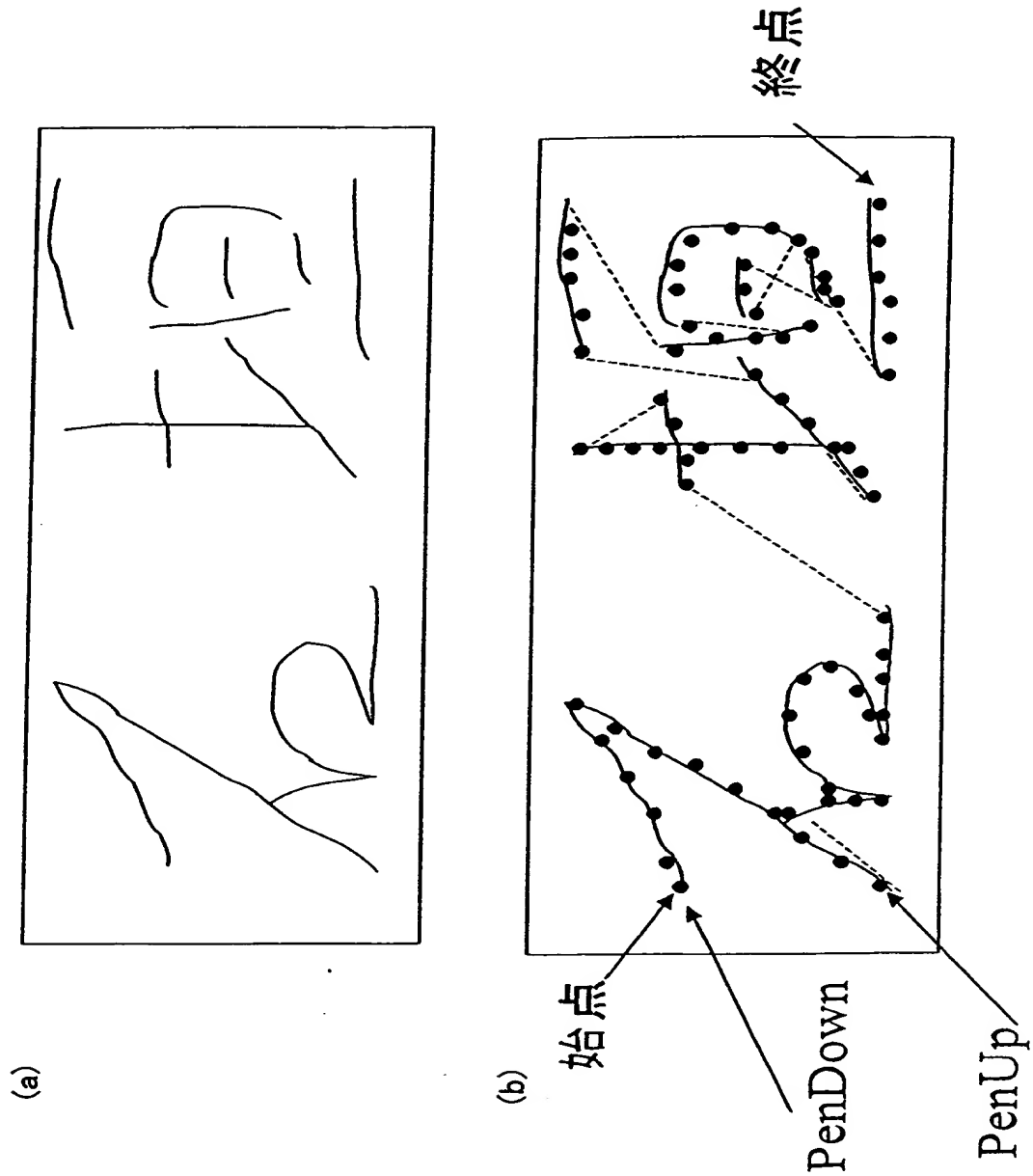
１００５　コンピュータのハードディスクやＲＡＭ等の記録媒体

【書類名】　　図面

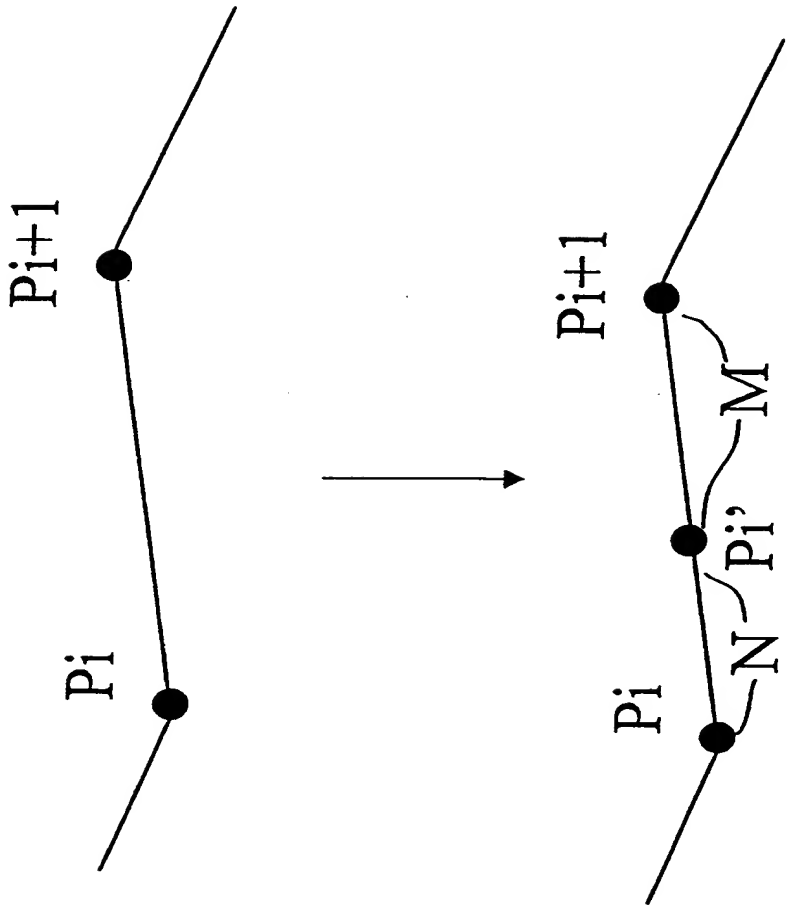
【図１】


100
電子サイン管理サーバ
110
データ送受信部
150
電子透かし付与部
151
電子透かし情報取得部
152
電子サインデータ要約処理部
153
電子透かし付与処理部
154
利用者確認部
160
商取引管理データ格納部
200
決済機関のサーバ
210
商取引情報生成部
300
400
利用者の携帯端末
11
取引内容入力部
10
業者端末
60
データ送受信部
40
制御部
50
商取引データ格納部
20
利用者識別情報読み取り部
30
手書きサイン入力部
31
商取引情報提示部

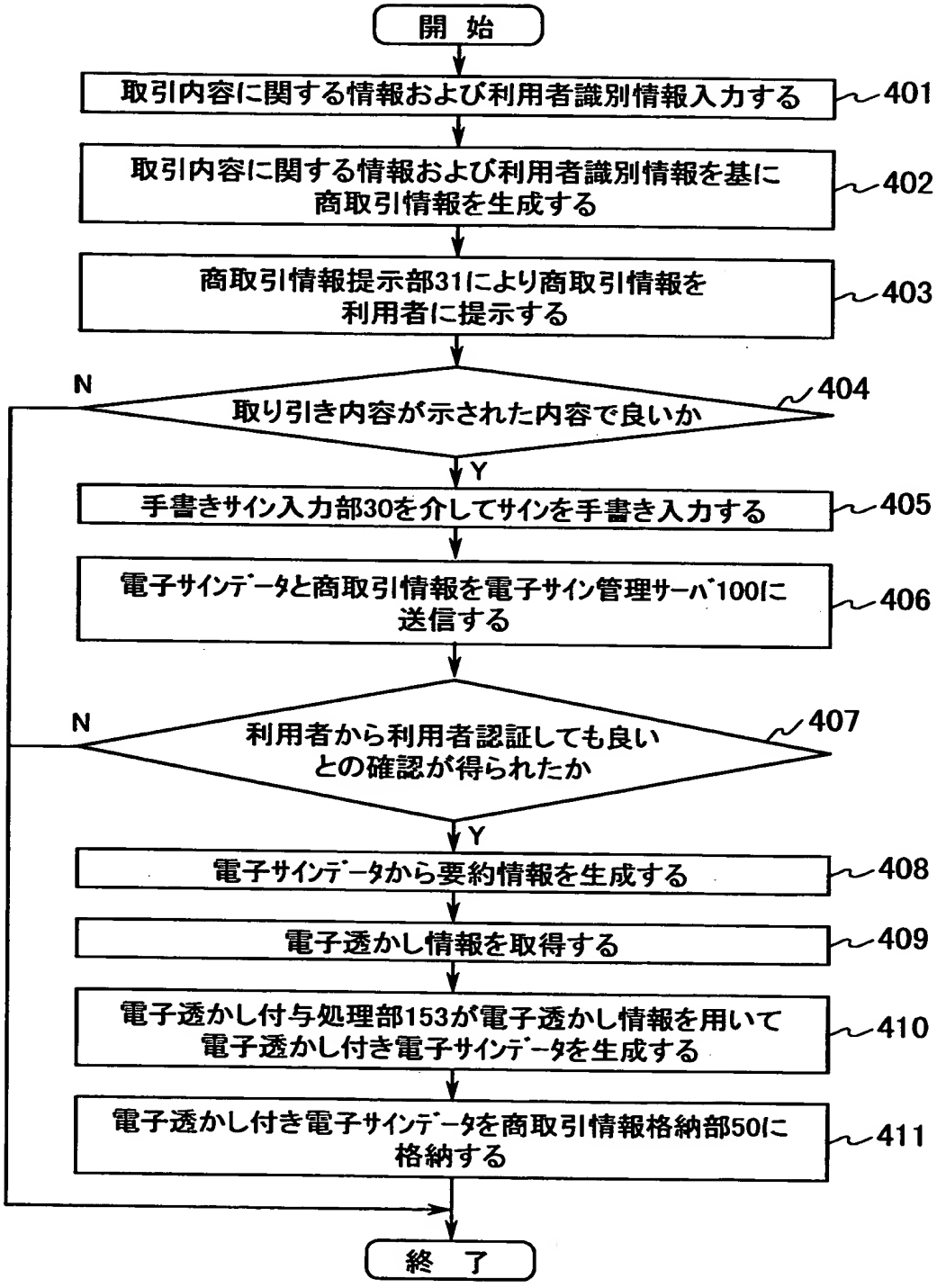
【図２】



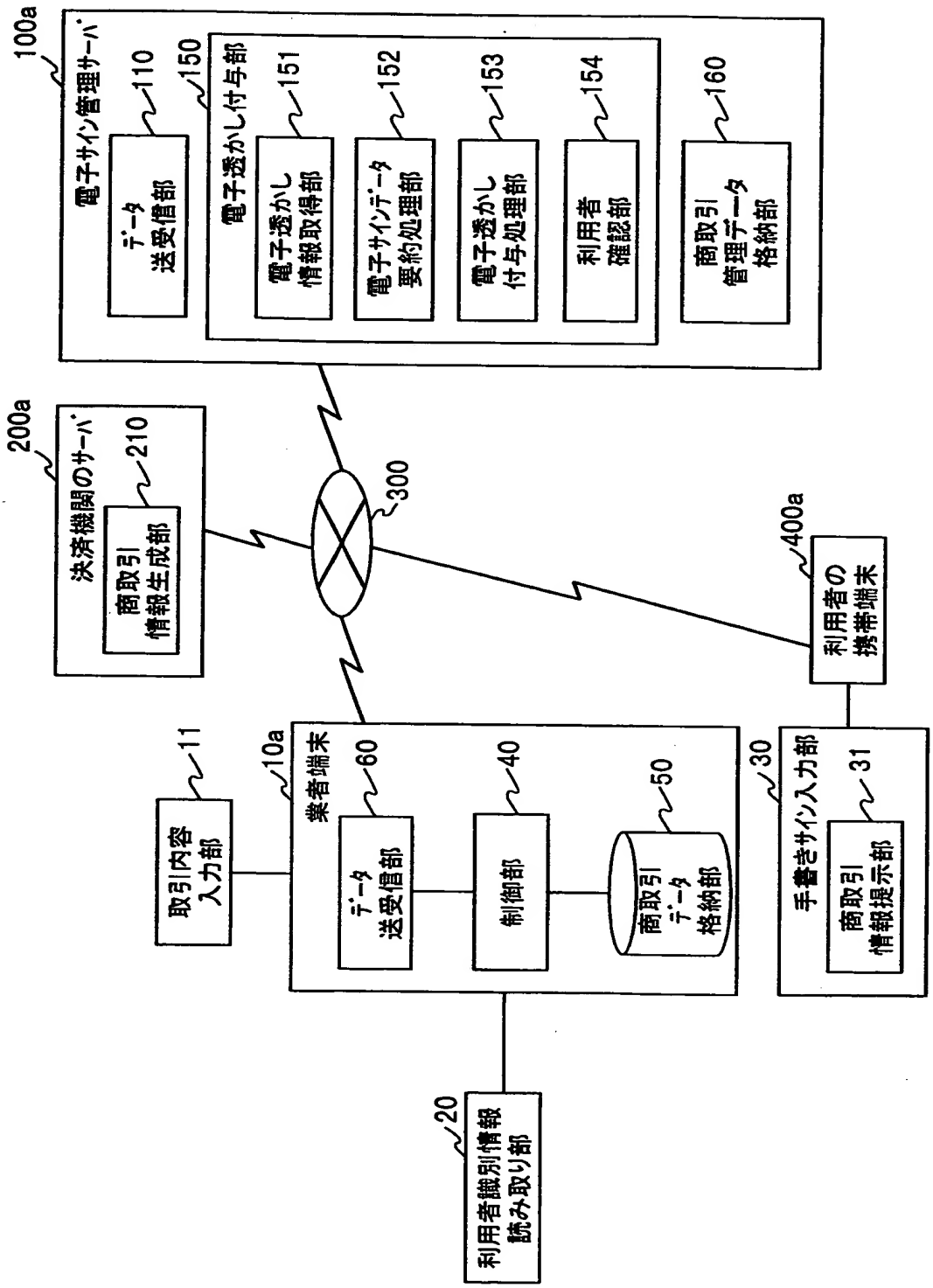
【図３】



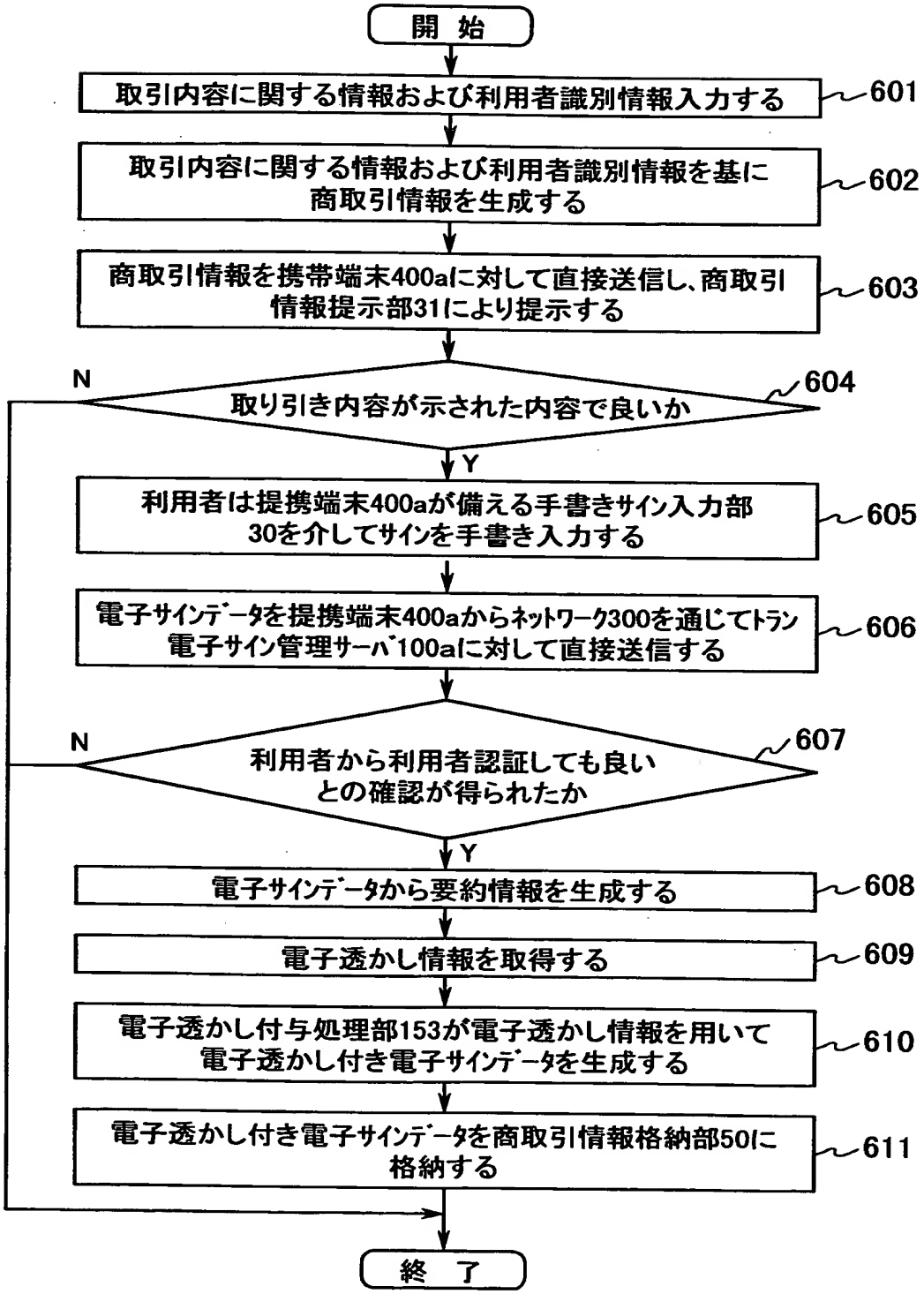
【図４】


開 始
取引内容に関する情報および利用者識別情報入力する
401
取引内容に関する情報および利用者識別情報を基に
商取引情報を生成する
402
商取引情報提示部31により商取引情報を
利用者に提示する
403
N
取り引き内容が示された内容で良いか
404
Y
手書きサイン入力部30を介してサインを手書き入力する
405
電子サインデータと商取引情報を電子サイン管理サーバ100に
送信する
406
N
利用者から利用者認証しても良い
との確認が得られたか
407
Y
電子サインデータから要約情報を生成する
408
電子透かし情報を取得する
409
電子透かし付与処理部153が電子透かし情報を用いて
電子透かし付き電子サインデータを生成する
410
電子透かし付き電子サインデータを商取引情報格納部50に
格納する
411
終 了

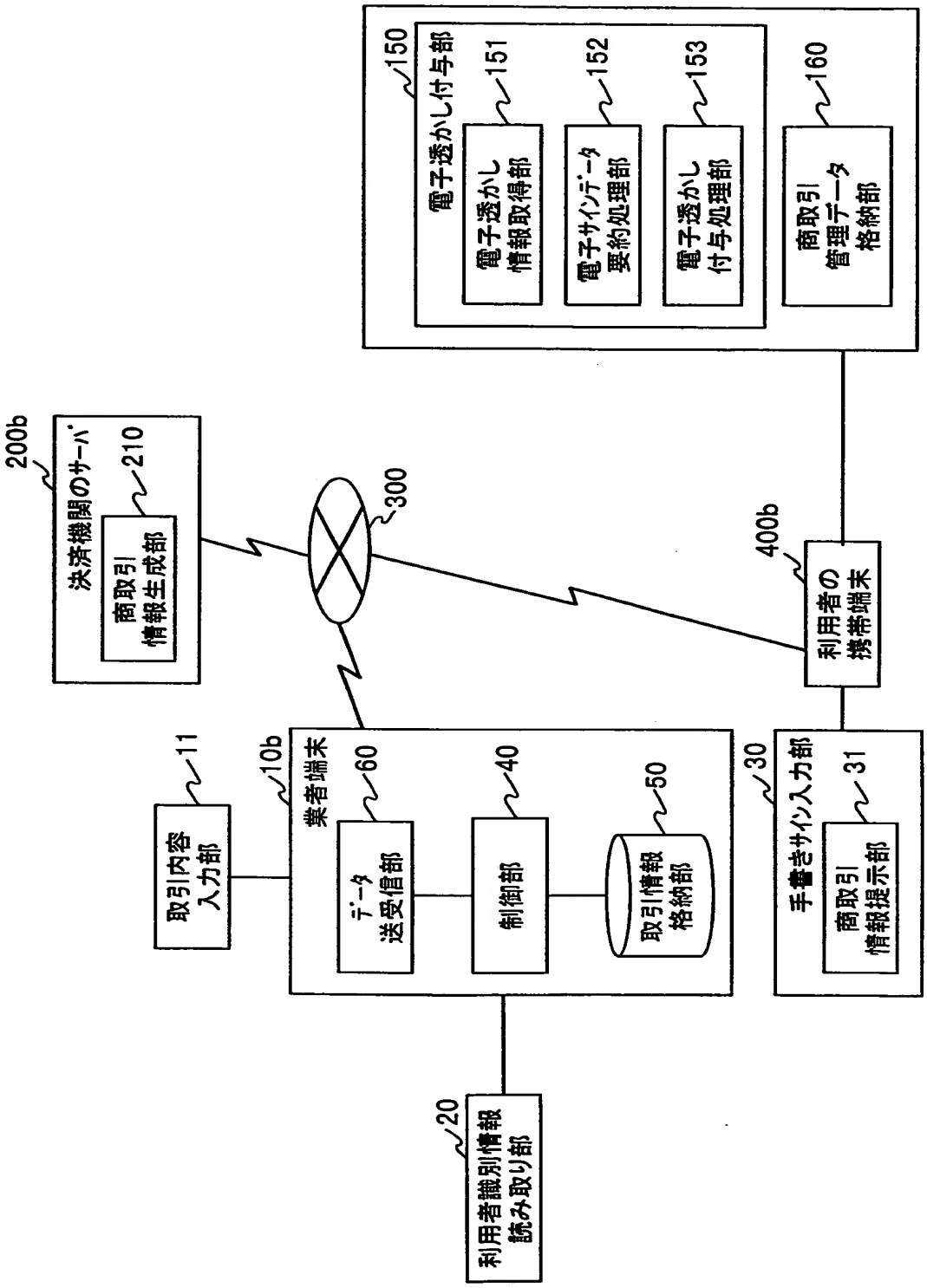
【図５】


100a
電子サイン管理サーバ
110
データ送受信部
150
電子透かし付与部
151
電子透かし情報取得部
152
電子サインデータ要約処理部
153
電子透かし付与処理部
154
利用者確認部
160
商取引管理データ格納部
200a
決済機関のサーバ
210
商取引情報生成部
300
400a
利用者の携帯端末
11
取引内容入力部
10a
業者端末
60
データ送受信部
40
制御部
50
商取引データ格納部
30
手書きサイン入力部
31
商取引情報提示部
20
利用者識別情報読み取り部

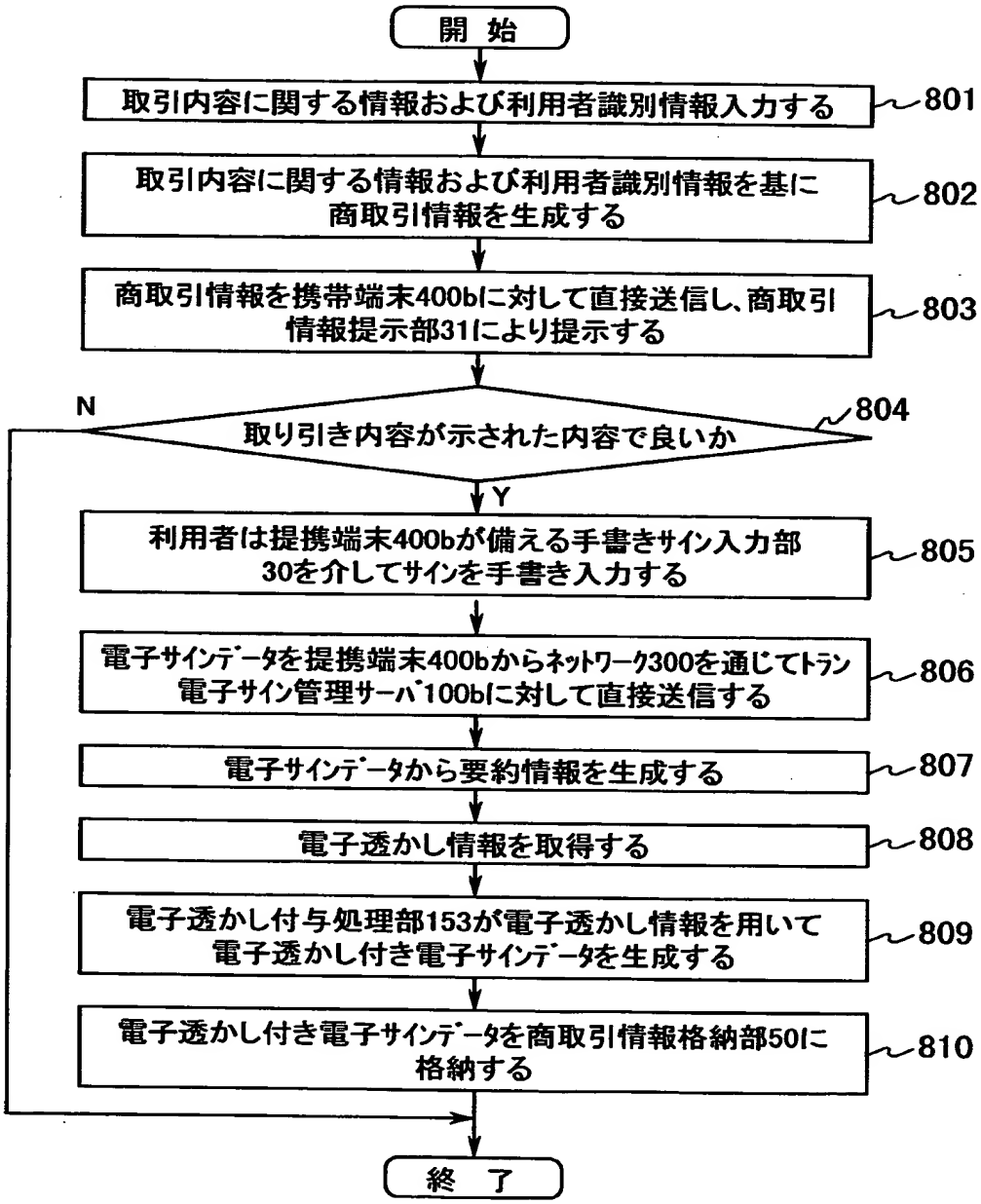
【図６】


開 始
取引内容に関する情報および利用者識別情報入力する
601
取引内容に関する情報および利用者識別情報を基に商取引情報を生成する
602
商取引情報を携帯端末400aに対して直接送信し、商取引情報提示部31により提示する
603
N
取り引き内容が示された内容で良いか
604
Y
利用者は提携端末400aが備える手書きサイン入力部30を介してサインを手書き入力する
605
電子サインデータを提携端末400aからネットワーク300を通じてトラン電子サイン管理サーバ100aに対して直接送信する
606
N
利用者から利用者認証しても良いとの確認が得られたか
607
Y
電子サインデータから要約情報を生成する
608
電子透かし情報を取得する
609
電子透かし付与処理部153が電子透かし情報を用いて電子透かし付き電子サインデータを生成する
610
電子透かし付き電子サインデータを商取引情報格納部50に格納する
611
終 了

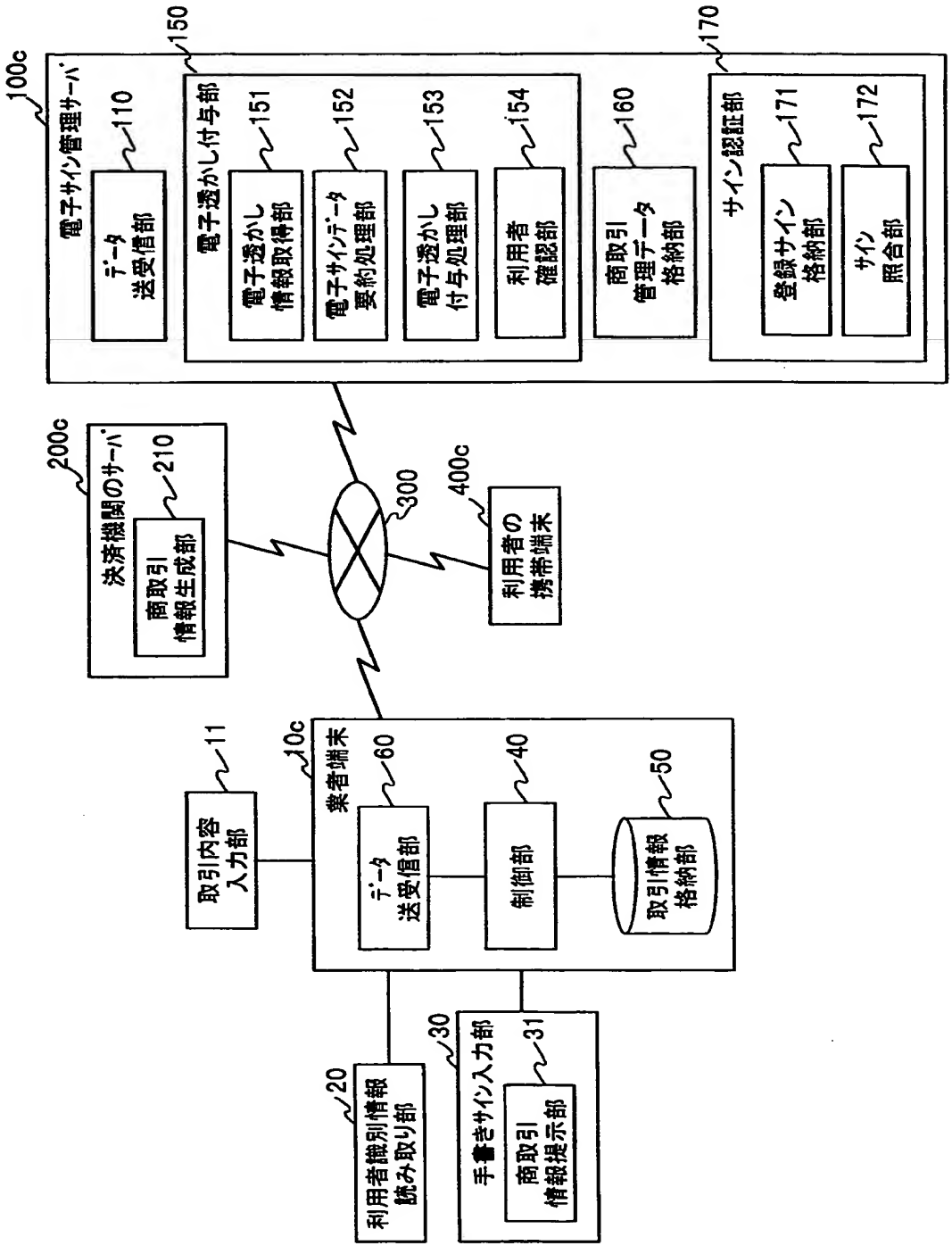
【図７】


150
電子透かし付与部
151
電子透かし情報取得部
152
電子サインデータ要約処理部
153
電子透かし付与処理部
160
商取引管理データ格納部
200b
決済機関のサーバ
210
商取引情報生成部
300
400b
利用者の携帯端末
11
取引内容入力部
10b
業者端末
60
データ送受信部
40
制御部
50
取引情報格納部
30
手書きサイン入力部
31
商取引情報提示部
20
利用者識別情報読み取り部

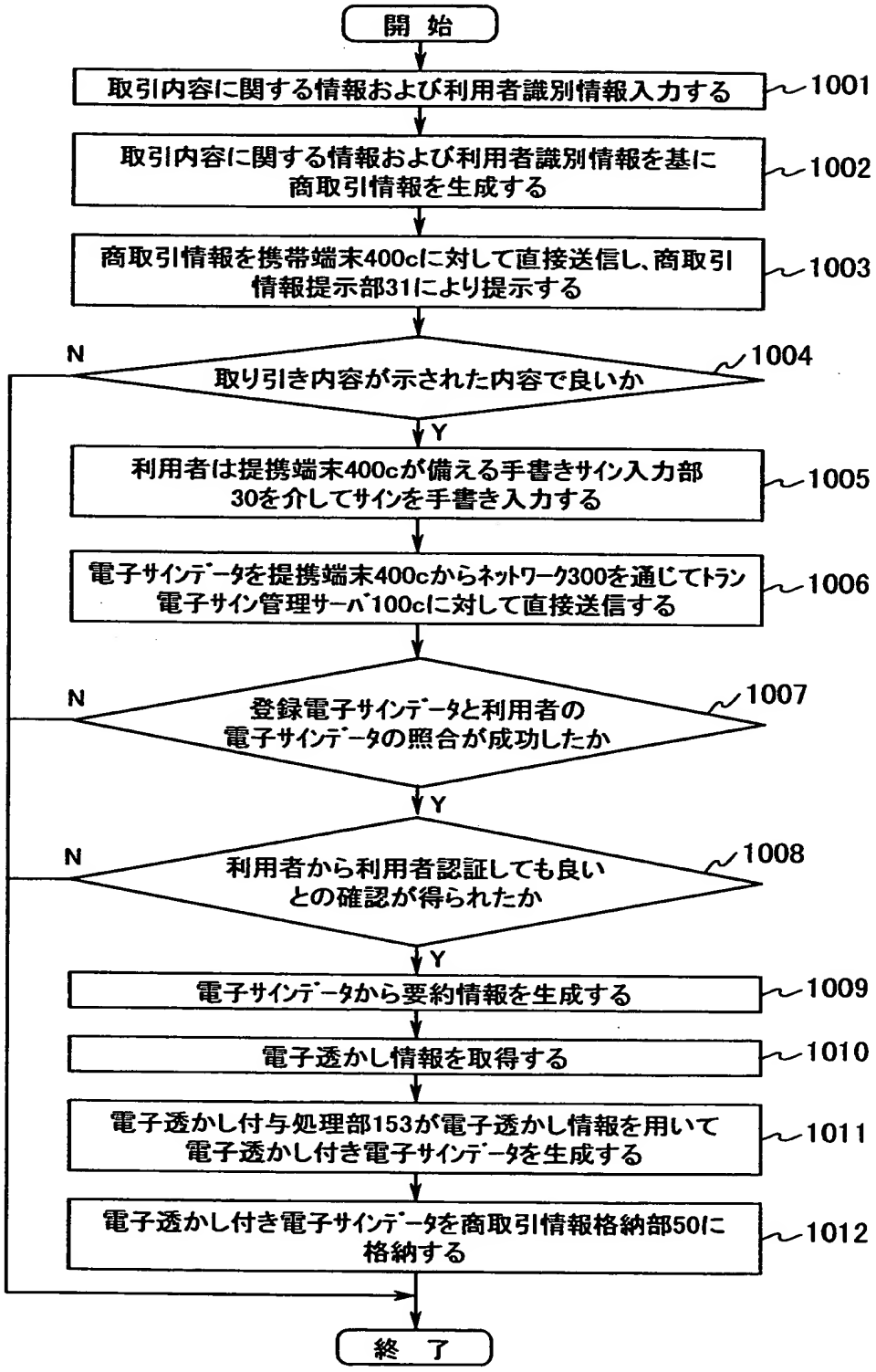
【図８】


開 始
取引内容に関する情報および利用者識別情報入力する
801
取引内容に関する情報および利用者識別情報を基に商取引情報を生成する
802
商取引情報を携帯端末400bに対して直接送信し、商取引情報提示部31により提示する
803
N
取り引き内容が示された内容で良いか
804
Y
利用者は提携端末400bが備える手書きｻｲﾝ入力部30を介してｻｲﾝを手書き入力する
805
電子ｻｲﾝﾃﾞｰﾀを提携端末400bからﾈｯﾄﾜｰｸ300を通じてﾄﾗﾝ電子ｻｲﾝ管理ｻｰﾊﾞ100bに対して直接送信する
806
電子ｻｲﾝﾃﾞｰﾀから要約情報を生成する
807
電子透かし情報を取得する
808
電子透かし付与処理部153が電子透かし情報を用いて電子透かし付き電子ｻｲﾝﾃﾞｰﾀを生成する
809
電子透かし付き電子ｻｲﾝﾃﾞｰﾀを商取引情報格納部50に格納する
810
終 了

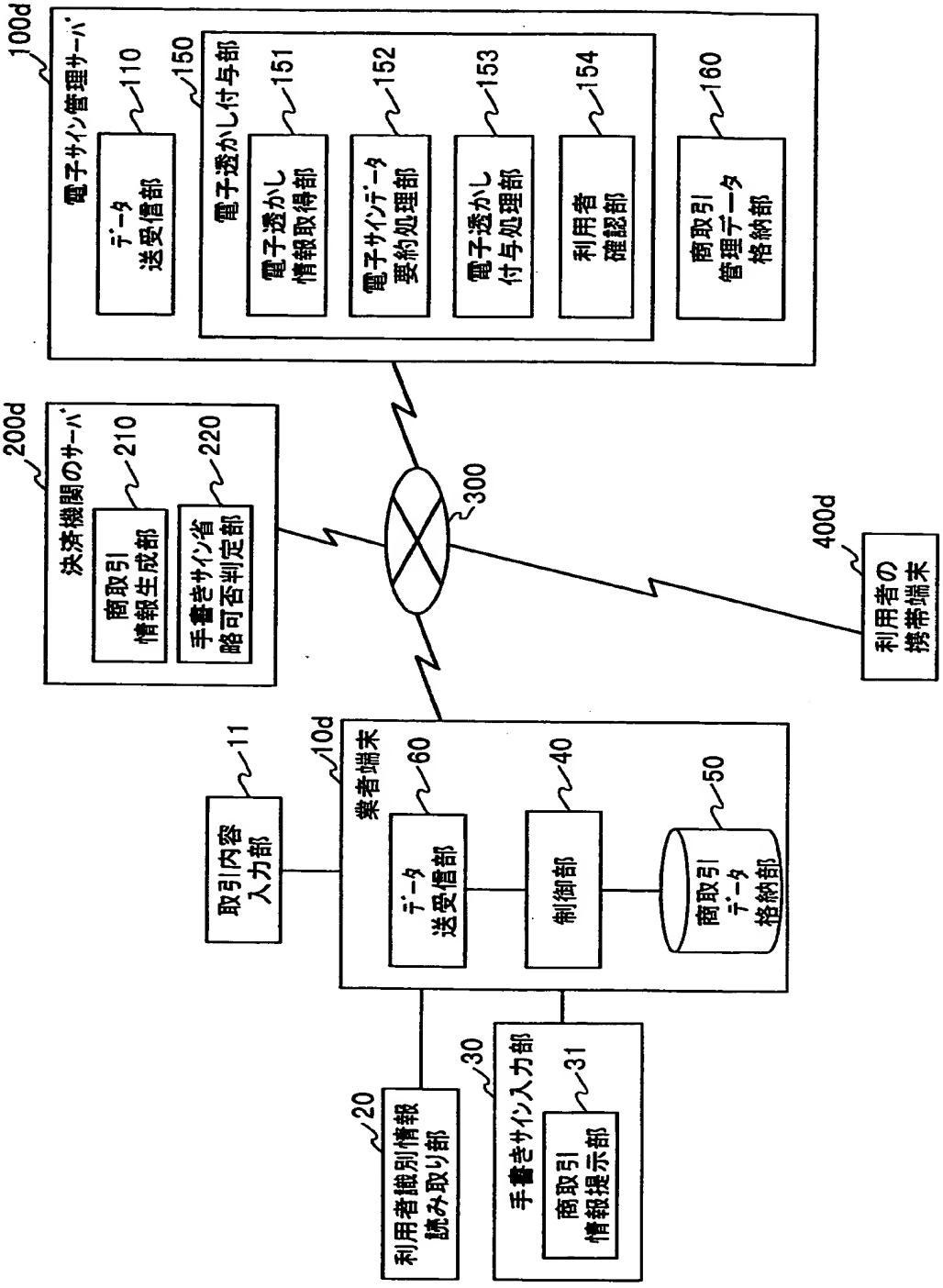
【図９】


100c
電子サイン管理サーバ
110
データ送受信部
150
電子透かし付与部
151
電子透かし情報取得部
152
電子サインデータ要約処理部
153
電子透かし付与処理部
154
利用者確認部
160
商取引管理データ格納部
170
サイン認証部
171
登録サイン格納部
172
サイン照合部
200c
決済機関のサーバ
210
商取引情報生成部
300
400c
利用者の携帯端末
11
取引内容入力部
10c
業者端末
60
データ送受信部
40
制御部
50
取引情報格納部
20
利用者識別情報読み取り部
30
手書きサイン入力部
31
商取引情報提示部

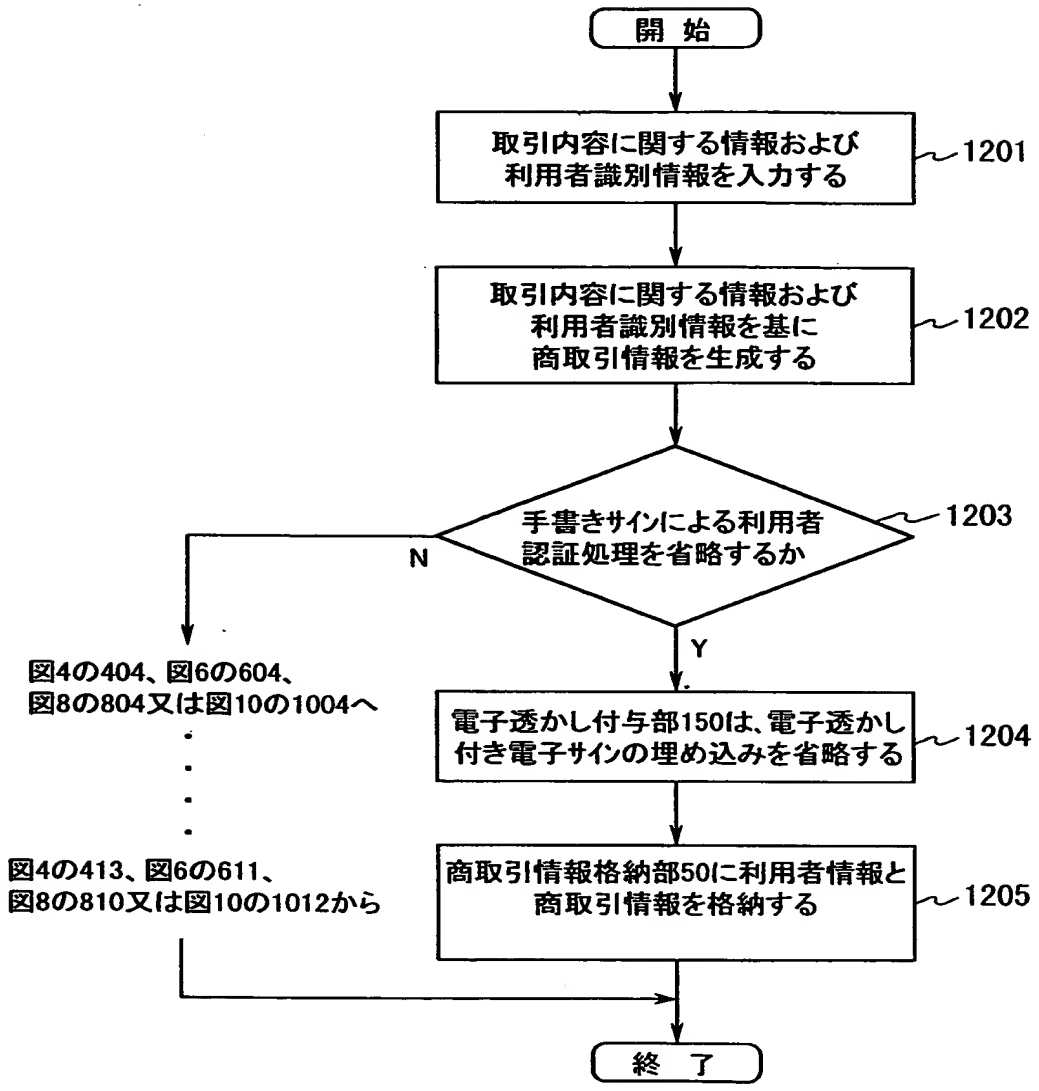
【図１０】


開 始
取引内容に関する情報および利用者識別情報入力する
1001
取引内容に関する情報および利用者識別情報を基に商取引情報を生成する
1002
商取引情報を携帯端末400cに対して直接送信し、商取引情報提示部31により提示する
1003
N
取り引き内容が示された内容で良いか
1004
Y
利用者は提携端末400cが備える手書きサイン入力部30を介してサインを手書き入力する
1005
電子サインデータを提携端末400cからネットワーク300を通じてトラン電子サイン管理サーバ100cに対して直接送信する
1006
N
登録電子サインデータと利用者の電子サインデータの照合が成功したか
1007
Y
N
利用者から利用者認証しても良いとの確認が得られたか
1008
Y
電子サインデータから要約情報を生成する
1009
電子透かし情報を取得する
1010
電子透かし付与処理部153が電子透かし情報を用いて電子透かし付き電子サインデータを生成する
1011
電子透かし付き電子サインデータを商取引情報格納部50に格納する
1012
終 了

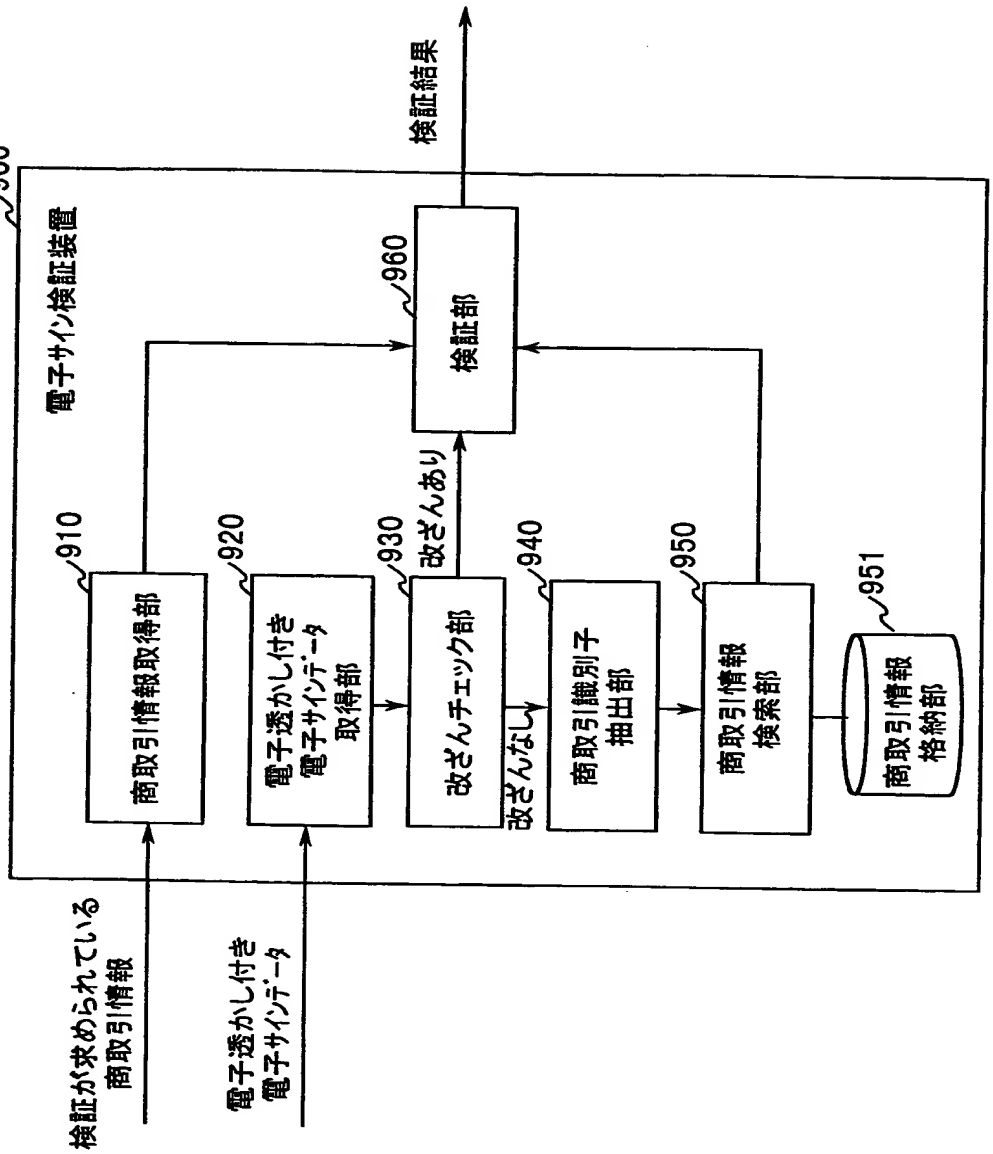
【図１１】


100d
電子サイン管理サーバ
110
データ送受信部
150
電子透かし付与部
151
電子透かし情報取得部
152
電子サインデータ要約処理部
153
電子透かし付与処理部
154
利用者確認部
160
商取引管理データ格納部
200d
決済機関のサーバ
210
商取引情報生成部
220
手書きサイン省略可否判定部
300
400d
利用者の携帯端末
11
取引内容入力部
10d
業者端末
60
データ送受信部
40
制御部
50
商取引データ格納部
20
利用者識別情報読み取り部
30
手書きサイン入力部
31
商取引情報提示部

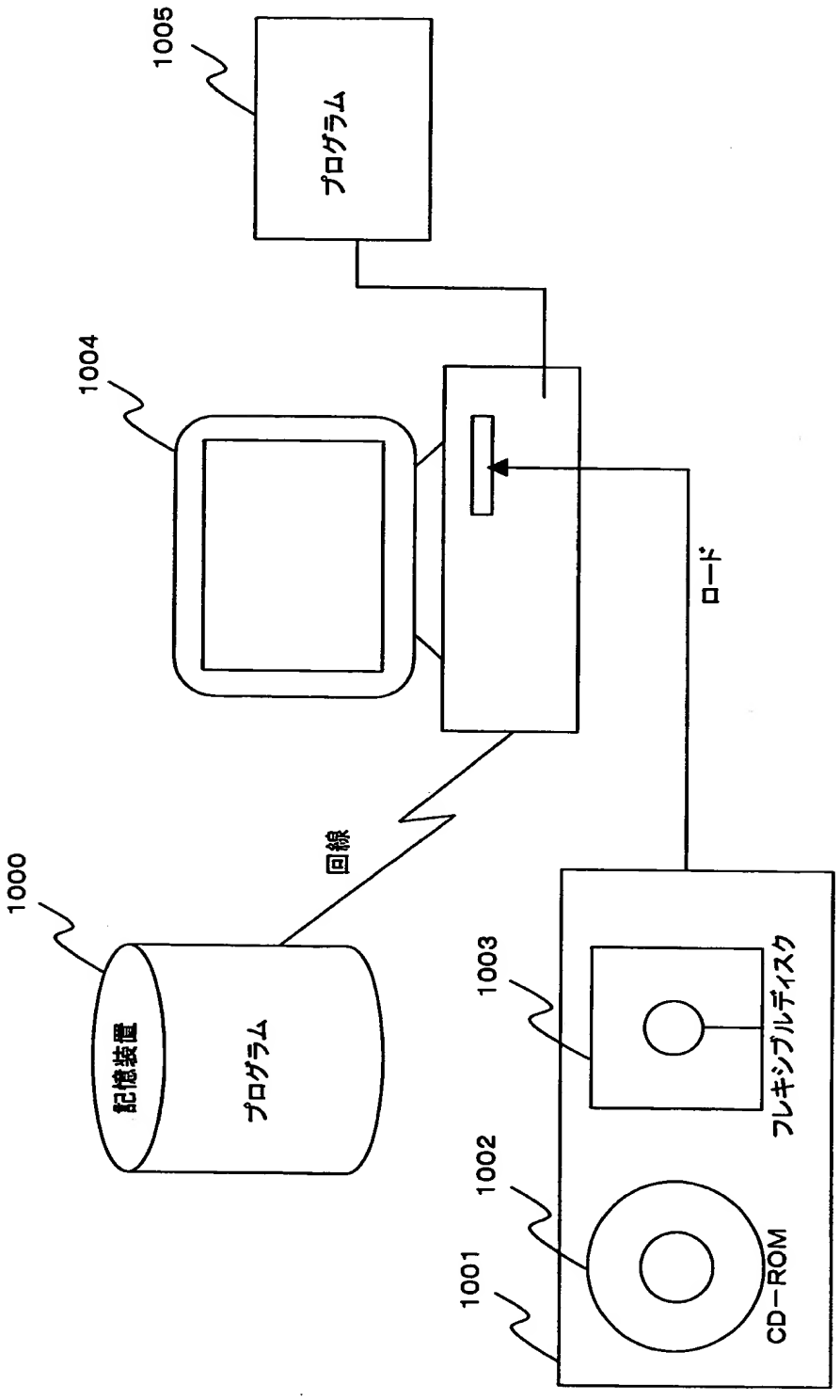
【図１２】


開 始
取引内容に関する情報および
利用者識別情報を入力する
1201
取引内容に関する情報および
利用者識別情報を基に
商取引情報を生成する
1202
手書きサインによる利用者
認証処理を省略するか
1203
N
Y
図4の404、図6の604、
図8の804又は図10の1004へ
電子透かし付与部150は、電子透かし
付き電子サインの埋め込みを省略する
1204
図4の413、図6の611、
図8の810又は図10の1012から
商取引情報格納部50に利用者情報と
商取引情報を格納する
1205
終 了

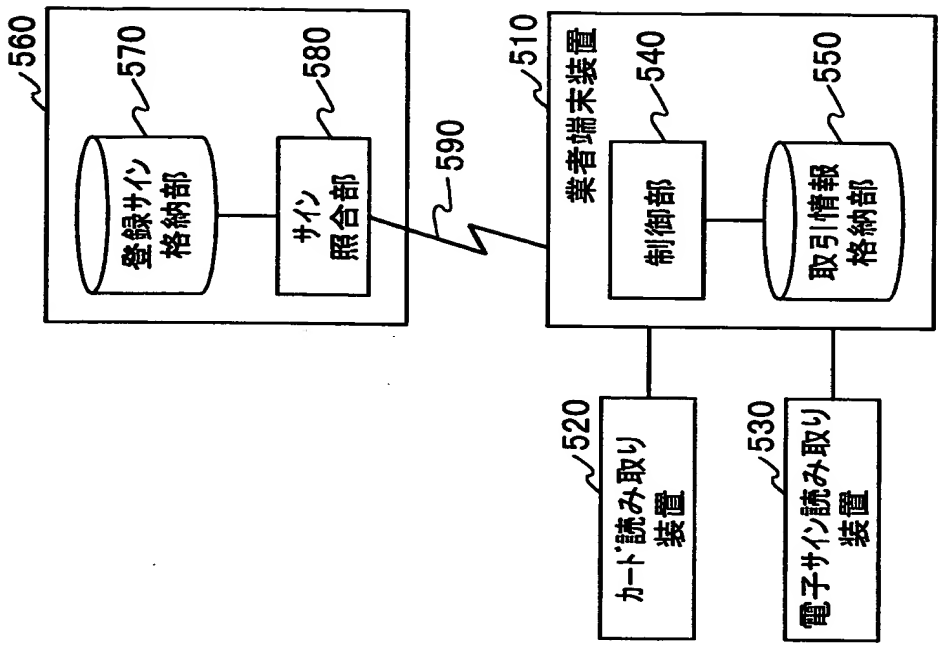
【図１３】


900
電子サイン検証装置
検証結果
960
検証部
910
商取引情報取得部
920
電子透かし付き
電子サインデータ
取得部
930
改ざんチェック部
改ざんあり
改ざんなし
940
商取引識別子
抽出部
950
商取引情報
検索部
951
商取引情報
格納部
検証が求められている
商取引情報
電子透かし付き
電子サインデータ

【図１４】


1005
プログラム
1004
ロード
回線
1000
記憶装置
プログラム
1003
フレキシブルディスク
1002
CD-ROM
1001

【図１５】


560
570
登録サイン格納部
580
サイン照合部
590
510
業者端末装置
540
制御部
550
取引情報格納部
520
カード読み取り装置
530
電子サイン読み取り装置

【書類名】　要約書

【要約】

【課題】　電子サインの取引業者による偽造、架空取引などへの流用を効果的に防止できる電子商取引システムおよび方法を提供する。

【解決手段】　取引内容入力部１１と利用者識別情報読み取り部２０から取引情報と利用者識別情報が入力され、決済機関のサーバ２００に送られ、商取引情報生成部２１０により商取引情報が生成される。利用者は商取引情報提示部３１を介して提示された取引内容を確認し手書きサイン入力部３０からサインを入力する。電子サインデータと商取引情報は電子サイン管理サーバ１００に送信され、サイン照合部１３０による電子サインデータの照合の後、電子サインデータの要約情報と取引内容を特定する商取引識別子とを電子透かし情報として付加し、電子透かし付き電子サインデータを生成する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社